HEADQUARTERS
UNITED STATES EUROPEAN COMMAND
UNIT 30400 BOX 1000
APO AE 09131

DIRECTIVE 1 July 2002
NUMBER 25-5

SECURITY

INFORMATION ASSURANCE

1. **Summary.** To provide USEUCOM and its Components and supporting elements with policy and guidance for the execution of Information Assurance (IA).

2. **Applicability**. This directive applies to all elements in USEUCOM to include HQ USEUCOM, USAREUR, USAFE, NAVEUR, MARFOREUR, DISA-EUR and SOCEUR; all USEUCOM-led Joint Task Forces (JTF) and Combined Joint Task Forces (CJTF), as well as supporting-CINC elements operating in the USEUCOM Area of Responsibility (AOR) regardless of administrative chain of command. This document will use the term “Components and supporting elements” to represent the preceding list of components, JTFs, agencies and elements. This document applies to all classifications and categories of information not addressed by superseding directives.

3. **Internal Control System**. This directive contains internal control provisions and is subject to the requirements of the internal management control program. For HQ USEUCOM and subordinate joint activities, the applicable internal control directive is ED 50-8, Internal Management Control Program.

4. **Suggested Improvements**. The proponent for this document is HQ USEUCOM, ECJ6-I. Suggestions for improvements, changes, and corrections should be addressed to HQ USEUCOM, Attn: ECJ6-I, Unit 30400, APO AE 09131.

5. **Cancellation**: USEUCOM Directive 25-5, 01 March 1999, “Information Assurance” is cancelled.

6. **References**. See Appendix A.

7. **Definitions**. See Appendix N.

8. **General**. Information transiting the DoD Global Information Grid (GIG) must be authentic, accurate, current, confidential, and available when needed. These requirements must be met by a reliable, interoperable infrastructure supporting the provisions of data integrity, authentication of remote users, confidentiality, and non-repudiation services. Due to the nature of interconnected networks, a risk assumed by one at any level is a risk assumed by all. In the USEUCOM AOR,

Information Assurance (IA) processes must be integrated across Service lines and IA measures must be coherently applied to all networks and elements. To achieve such cohesion, it is vitally important for all USEUCOM-tenant organizations to ensure IA policies and procedures reflect an active coordination and review process.

9. **Responsibilities**.

a. HQ USEUCOM ECJ6-I, Information Assurance (IA) Division:

(1). Develops IA doctrine, strategy, and policy for USEUCOM contingency plans, operations plans, JTF exercise plans, and daily operations.

(2). Assists the EUCOM Theater C4ISR Coordination Center (TCCC) by providing situational awareness of the security posture of the theater communications infrastructure.

(3). Assists the JTF Staff with Information Assurance implementation through Defense in Depth, Communications Security (to include communication monitoring), information systems certification and accreditation, and risk mitigation.

(4). Provides the J6 representative to the HQ EUCOM Information Operations Cell (J39).

(5). Functions as the Command subject-matter expert for Information Assurance doctrine and policy, and coordinates with the Joint Staff, Services, and Agencies on IA matters impacting upon operational readiness.

(6.) Functions as the technical and security advisor to the HQ USEUCOM Designated Approving Authority (DAA).

(7). Manages the Certification and Accreditation program for HQ USEUCOM, and represents the DAA in all working forums.

(8). Works with counterpart IA policy and DAA offices in NATO and coalition-partner governments to facilitate secure interoperability across C4I systems.

(9). Analyzes IA Command-wide threats and vulnerabilities, and identifies protection levels required for USEUCOM portions of the GIG.

(10). Conducts the HQ USEUCOM information protection, education, training and awareness program.

(11). Identifies critical points of failure and other potential vulnerabilities within the theater communications infrastructure, and recommends protective measures.

(12). Identifies CERT, network operations centers, and other organizational functions required to coordinate and direct IA protective measures, and implement theater-wide Information Assurance through Defense in Depth.

(13). Coordinates Joint COMSEC Monitoring Activity (JCMA) support for USEUCOM or component-sponsored operations and exercises.

(14). Functions as the theater Key Management Infrastructure (KMI) Office and major operational COMSEC authority for joint cryptographic applications in USEUCOM.

(15). Provides representation to Service, agency, and NATO IA working groups to include those working groups and committees engaged in theater Key Management Infrastructure (KMI) procurement and development efforts.

(16) Provides comprehensive planning and programming of theater IA requirements and advocates for development of theater IA resources through the CINC's Integrated Priority List (IPL), the Joint Monthly Readiness Review process, and the J6 500-day plan.

b. HQ USEUCOM ECJ6-O, Communications Operations Division:

(1). Establishes and operates the EUCOM Theater C4ISR Coordination Center (TCCC) through which IA matters and incidents are coordinated throughout the theater.

c. HQ USEUCOM ECJ39, Information Operations (IO) Division:

(1). Through the Computer Network Defense (CND) IO Cell and IO Working Group (IOWG), coordinates with ECJ6-I on all operational IA matters and requirements impacting upon the command and control of U.S. forces in the USEUCOM AOR.

(2). Coordinates J3 approval theater JCMA requirements and actions taken to mitigate poor Operational Security (OPSEC) practices discovered via the JCMA.

d. NSA Central Security Service Europe (NCEUR):

(1). Coordinates with ECJ6-I on all national level IA guidance and policy.

(2). Facilitates all interactions between ECJ6, ECJ39 and JCMA.

(3). Provides technical guidance on INFOSEC hardware.

(4). In cooperation with ECJ2, provides threat information relative to communications and information systems supporting USEUCOM.

(5). Facilitate NSA "Blue Team" network evaluations and "Red Team" network assessments of EUCOM Headquarters, Component and supporting element networks.

e. All Components and supporting elements, agencies and other supporting entities to include DISA-EUR, USAREUR, NAVEUR, USAFE, MARFOREUR, SOCEUR shall:

(1) Execute USEUCOM policies and security requirements to ensure resources sufficient to secure USEUCOM information and information systems throughout the USEUCOM Area of Responsibility (AOR).

(2) Integrate IA into relevant policies and guidance.

(3) Integrate IA into OPLANS and Exercises.

(4) Comply with all policy in this directive.

FOR THE COMMANDER IN CHIEF:

OFFICIAL:

DANIEL J. PETROSKY
Lieutenant General, USA
Chief of Staff

AVA N. WEBB-SHARPLESS
LTC, USAF
Adjutant General

APPENDIXES:

- A - References
- B - Defense in Depth
- C - Information Systems Personnel Appointment and Training
- D - Accreditation
- E - Markings
- F - Media Reuse
- G – Deployed Information Assurance
- H - Information Conditions (INFOCONs)
- I - Communications Security Release to Foreign Nations
- J - Joint Key Management
  ANNEX A to APPENDIX J - Sample COMSEC Alert Message
- ANNEX B to APPENDIX J - Sample COMSEC Appendix
- K - The DoD Public Key Infrastructure
- L - Information Assurance Vulnerability Assessment (IAVA) Process
- M – Terms and Definitions

DISTRIBUTION:
P

Appendix A

References

A - 1. DoD CIO Guidance and Policy Memorandum 10-8460, “Network Operations”, 22 Aug 2000.

A - 2. Deputy Secretary of Defense (DEPSECDEF) Memorandum “DoD Information Assurance Vulnerability Assessment”, 31 Dec 99.

A - 3. ASDC3I letter, "Secret and Below (SABI) Reaffirmation Policy.", 11 May 1998.

A - 4. ASDC31 Memo, 7 November 2000, "Policy Guidance for use of Mobile Code Technologies in Department of Defense (DoD) Information systems.

A - 5. ASDC3I Memorandum “Removal of Personally Identifying Information of DoD Personnel from Unclassified Web Sites”, 28 Dec 01

A - 6. CJCSI 3320.03, "Joint Communications Electronics Operation Instructions," 1 Jan 1999.

A - 7. CJCSI 6110.01, "CJCS-Controlled Tactical Communications Assets," 25 Jan 1996.

A - 8. CJCSI 6010.01A, "Coordination of United States Command, Control, Communications, and Computer Systems Positions in International Forums," 16 Jan 1998.

A - 9. CJCSI 6211.02A, "Defense Information System Network and Connected Systems," 22 May 1996.

A - 10. CJCSI 6212.01B, "Interoperability and Supportability of National Security Systems, and Information Technology Systems," 8 May 2000.

A - 11. CJCSI 6215.01, "Policy For The Defense Switched Networks," 1 Feb 1995.

A - 12. CJCSI 6250.01, "Satellite Communications," 20 Oct 1998.

A - 13. CJCSI 6510.01C, "Information Assurance and Computer Network Defense," 1 May 2001.

A - 14. CJCSI 6510.02A, "Communications Security (COMSEC) Modernization Plan," 30 Nov 1999.

A - 15. CJCSI 6510.06, "Communications Security Releases to Foreign Nations," 15 Feb 2001.

A - 16. CJCSI 6740.01, "Military Telecommunications Agreement and Arrangements Between The United States and Regional Defense Organizations or Friendly Foreign Nations," 18 Sep 1996.

A - 17. CJCSM 3113.01A, "Theater Engagement Planning," 31 May 2000

A - 18. CJCSM 3122.03A, "Joint Operation Planning and Execution System, Volume II, Planning Formats and Guidance," 31 Dec 99.

A - 19. CJCSM 3141.01A, "Procedures For The Review of Operation Plans," 15 Sep 1998.

A - 20. CJCSM 5222.01, "National Military Command System Security Classification Manual," 15 Jan 1997.

A - 21. CJCSM 6120.01A, "Joint Multi -Tactical Digital Information Link (TADIL) Operating Procedures," 24 Oct 1997.

A - 22. CJCSM 6230.05, "Joint Have Quick Planners Manual," 15 May 1996.

A - 23. CJCSM 6231.05A, "Joint Communications Security," 2 Nov 1998.

A - 24. CJCSM 6231.07B, "Joint Network Management and Control," 31 Dec 1999.

A - 25. DoD Directive O-8530.1" Computer Network Defense (CND)", 8 Jan 2001

A - 26. DoD Directive 3020.26 "Continuity of Operations (COOP) Policy and Planning", 26 May 1995

A - 27. DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," 30 Dec 1997.

A - 28. DoD IOMP (Information Operations Master Plan), October 1998.

A - 29. DoD 5105.21-M-1, "Sensitive Compartmented Information Administrative Security Manual," August 1998.

A - 30. DoD 4640.6, "Communications Security Telephone Monitoring and Recording," June 26, 1981

A - 31. DoD 5000.1, "The Defense Acquisition System," October 23, 2000

A - 32. DoD 5010.38, "Internal Management Control Program," July 16, 1984

A - 33. DoD 5025.1-M, "DoD Directives System Procedures," August 1994

A - 34. DoD 5137.1, "Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD (C3i))," February 12, 1992

A - 35. DoD 5200.1, "Information Security Program," 13 Dec 1996

A - 36. DoD 5200.2, "DoD Personnel Security Program," December 20, 1979

A - 37. DoD 5200.28, "Security Requirements for Automated Information systems," March 21, 1988.

A - 38. DoD 5230.9, “Clearance of DoD Information for Public Release”, 15 July 1999.

A - 39. IASE “SABI Referenced Implementations (SRI) Version 2.1”, 15 Jan, 02.

A - 40. INFOCON Levels and Directive Actions

A - 41. Joint Inter-theater COMSEC Package (JICP), JCMO Redbook and Status Messages.

A - 42. JP 3-13, "Joint Doctrine for Information Operations," 9 Oct 1998.

A - 43. NAG-16/TSEC, Field Generation and Over-The-Air Distribution of COMSEC Key in Support of Tactical Operations and Exercises.

A - 44. NSTISSP No. 11, National Information Assurance Acquisition Policy.

A - 45. NSTISSI No. 4005, "Safeguarding Communications (COMSEC) Facilities and Materials," August 1997.

A - 46. NSTISSI No. 4009, "National Information Systems Security (INFOSEC) Glossary," January 1999.

A - 47. NSTISSI No. 7003, 7003 (C/NF), “Protected Distribution Systems”, 13 December 1996.

A - 48. USEUCOM TIAMP (Theater Information Assurance Master Plan), October 2000.

A - 49. X.509 Certificate Policy, (Certificate Policy for the United States Department of Defense), 13 Dec 1999.

A - 50. National Security Agency/V43 DoD Firewall Guidance (Version 1.2)

A - 51. DISN Connection Security Requirements, Nov 1997.

A - 52. Director of Central Intelligence Directive 1/21, Annex D, “Physical Security Standards for Sensitive Compartmented Information Facilities (SCIF)”, 29 July 1994.

Appendix B

Defense in Depth

B-1. **General**. The threat to information systems (a.k.a. Automated Information Systems or Communications-Computer Systems) and networks supporting USEUCOM is complex and covers a broad spectrum of potential sources to include hackers, disgruntled insiders, information warriors, foreign intelligence activities, terrorists, organized crime, and industrial espionage. The interconnection of the NIPRnet to the Internet and the reliance of our business practices on interaction with corporate entities in the greater Internet expose our military networks to these threats. All of these threats are exacerbated by careless or sloppy security behaviors of legitimate information system users. Defensive measures in support of Information Assurance are categorized into three categories: People, Technology and Operations. Defensive measures are implemented at varying levels creating enclaves and nested enclaves to ensure interlocking and overlapping defensive perimeters.

B-2. **People**:

a. Training and Awareness. A security training and awareness program shall be in place for all persons accessing Information systems. The program shall ensure that all persons responsible for information systems and/or information therein, and all persons who access information systems are aware of proper operational and security-related procedures and risks. Minimum requirements for security awareness training are as follows:

(1) The training shall be specific to the operational environment. Classroom training, video presentations, personalized instruction, Computer-Based Training, and read-and-sign briefings are all acceptable methods of presentation. More than one method of training is encouraged.

(2) Each individual shall receive training prior to being granted access to any information system and annual refresher training shall be conducted thereafter.

(3) Training records shall be maintained. At a minimum the records shall document that initial and annual refresher training was provided to each individual who has access to an information system.

b. All commands within USEUCOM shall have a documented training program for System Administrators IAW Appendix C “Security Manager Program”.

B-3. **Technology:** Defensive technology measures are applied at three levels: networks, enclave boundaries and local computing environments (internal to the enclave). This policy applies to garrison (Base/Post/Camp/Station) information systems as well as deployed information systems.

a. Networks. Networks are the interconnections between enclaves and are viewed as “untrusted” resources from the perspective of the enclave. Networks include, but are not limited to, NIPRNET and SIPRNET.

(1) Any Components and supporting elements that have direct control or authority over Networks supporting USEUCOM shall:

i. Have the capability to implement blocking or other protection methods at the network interconnect as directed by the USEUCOM J3 and in coordination with the TCCC and the Components and supporting elements.
ii. Ensure that redundant, multiple data paths exist for the transport of information to every extent possible IAW CJCSI 6510.01C.
iii. Employ Intrusion Detection devices on critical network paths as directed by USEUCOM J6.
iv. Employ TRANSEC measures IAW CJCSI 6511.01 and other applicable regulations.

(2) Memorandums of Agreement (MOA). The interconnection of networks under the security cognizance of different DAAs shall be documented in a MOA or similar agreement. Similarly, the interconnection of networks under the cognizance of the same DAA shall be documented in a security approval amending the security accreditation of each network. See Appendix D for more information on MOAs.

(3) Secret and Below Interoperability (SABI)/Top Secret and Below Interoperability (TSABI). All requirements to interconnect information systems operating at the SECRET level to information systems operating at a lower classification shall be submitted to the SABI process for engineering review and recommendation to the responsible DAA(s). Interconnections that include SCI level information systems are handled through a similar but separate process. HQ USEUCOM (ECJ6-I and ECJ6-TCCC) have been charged with maintaining high-level oversight over all interconnections between information systems of different security levels, regardless of security levels, operating in the USEUCOM AOR. For an application to be SABI/TSABI relevant, information must flow, at least one way, between the systems.

b. Enclave Boundaries. Enclave boundaries are the interconnection between an enclave (local computing environment) and an “untrusted” network or enclave. Enclave boundaries may be the network “De-Militarized Zone (DMZ)” for a Post/Base/Camp/Station or deployed location, the DISN NIPRNET CONUS Gateways, theater Internet Access Points (IAPs) or reachback to STEP Sites.

(1) Firewall technology shall be deployed at the enclave boundary on all Internet connections. Firewall technology is strongly recommended on all other connections. Firewall technology includes firewalls or routers that can be configured to block based on ports, protocols or addresses. Additional firewall configuration and administration guidance can be found in National Security Agency/V43 DoD Firewall Guidance (Version 1.2), and CJCSM 6510.01, Information Assurance (Defense-in-Depth), 30 March 2001. Implementation will be commensurate with risk and balanced with the operational impact to supported customers.

(2) Port/Protocol blocking shall be a capability at the enclave boundary. Port/protocol blocking shall be implemented commensurate with risk. All port/protocol blocking changes (implementation or removal) shall be coordinated with the TCCC.

(3) Intrusion Detection shall be deployed at the enclave boundary on all Internet connections. It is strongly recommended on all other connections. All interconnections between a classified information system and an information system of lower security level shall employ IDSs on both the "high" and "low" sides of the interconnecting security guard.

(4) E-mail attachment blocking shall be a capability at the enclave boundary if e-mail services are provided.

c. Enclave (Local Computing Environment). Enclaves or local computing environments are the physical or organizational environment under the control of a single authority with a common, uniform security policy. Enclaves are typically defined by geography (Base/Post/Camp/Station) but may also be defined operationally (i.e. JTF AFFOR or ARFOR networks) or logically (DMS). Enclaves are as big (i.e. DISN) or as small (i.e. deployed LAN) as the purview of the controlling authority. All Components and supporting elements shall define the enclaves and boundaries for the information systems under their control and/or responsibility. This includes the interconnect between the USEUCOM portion of the GIG and other networks (i.e. Internet Access Points, NIPRNET/SIPRNET Gateways, STEP sites).

(1) Malicious Logic Protection. All information systems shall employ DISA-approved virus protection software obtained from a DoD-approved source. At a minimum, anti-virus software shall be scheduled to run on all enclave information systems daily and all incoming e-mail and file transfers shall be scanned for malicious logic/viruses before use. Procedures shall be established to rapidly obtain, distribute and install changes to anti-virus software on all information systems. Virus prevention, detection, eradication, and reporting procedures shall be included in user awareness training. Viruses are a subset of malicious logic (e.g., virus, worm, Trojan horse, logic bomb, etc.) and current anti-virus tools are capable of detecting and eradicating most forms of malicious logic. USEUCOM encourages the use of DISA approved virus protection software for home use as well.

B-4. **Operations:** Operations are the policy, procedures and processes that ensure a secure execution of defense-in-depth. Operations policies are applicable to Networks, Enclaves and Local Computing Environments.

a. Configuration Management. Proper configuration management tools help to establish and maintain a security posture for networked systems (e.g., workstations, servers, mainframes, firewalls, routers, etc., and the software residing on them). Commands shall implement a configuration management program for each information system commensurate with the sensitivity, complexity, and mission criticality of the system. The program shall address all system elements, which enforce system-security policy. The objective of the configuration management program is two-fold: first, to provide a forum for evaluating the impact of proposed configuration changes on the system security profile; second, to provide a forum for tracking and resolving risk-management issues identified during system accreditation. To ensure the integrity of critical networked systems, distribution of hardware, firmware, and software shall be under configuration management control and shall be provided an appropriate level-of-protection to assure product integrity. The use of standardized automation tools to establish and enforce configuration management is encouraged. The system program office shall provide the Systems Security Authorization Agreement (SSAA) in accordance with DoD Instruction 5200.40, DITSCAP.

b. Device Access. Access to critical network and IA devices (routers, firewalls, IDSs, core servers, etc.) shall be restricted both physically and logically (i.e. remote access) to protect the critical network or IA device from malicious or non-malicious disruption. Access restriction shall be commensurate with risk.

c. Audit Logs. IA Device logs as well as information system audit logs shall be maintained for a minimum of one year. Additionally:

(1) All components and supporting elements shall specify a minimum audit log data-element set for correlating information system security incidents across multiple sites within the theater. This minimum data-element set shall be implemented in all information systems. DAA's may specify additional data collection requirements.

(2) Audit log reduction and analysis (ARA) shall, wherever possible, be migrated to a single, protected environment. The migration of ARA processing to a single, protected environment allows increased incident correlation across multiple information systems within a site and across multiple sites within the theater.

(3) Audit logs shall be tailored to USEUCOM specific information and information systems.

d. Vulnerability Scans. Vulnerability scans shall be executed against the network, the enclave boundary and within the local computing environments semi annually at a minimum. The scan will include password compliance, unauthorized ports/service activation, and secure baseline compliance. All high and medium vulnerabilities will be corrected or documented and waived by the DAA within 60 days of identification.

e. Contingency Plans. Continuity of Operation Plans (COOP)/Contingency Plans shall be developed and maintained IAW DoD Directive 3020.26. The communications and information components of COOP plans shall be exercised yearly and the results of tests shall be documented.

f. Data Backup. Data backup and restoral plans shall be developed and executed to ensure safe, timely backup and restoral of USEUCOM information. Backup plans shall include periodicity of backups, operational impacts of backups and physical storage of backup media.

g. Network Connection to Non-DoD and Non-U.S. Activities. CJCSI 6211.02A, Defense Information System Network and Connected Systems, provides policy on the connection of non-DoD and non-U.S. activities to the GIG. In addition to meeting the access and connection requirements for non-DoD U.S. activities, use of DoD portions of the GIG by foreign governments and allied organizations shall be approved under the terms of CJCSI 6740.01, Military Telecommunications Agreement and Arrangements Between The United States and Regional Defense Organizations or Friendly Foreign Nations (Ref A-16). Approved foreign users are subject to the same user agreement as DoD users. ASDC3I letter of 11 May 1998, SABI Reaffirmation Policy (Ref A-3) requires using the SABI process for interconnections between systems/networks at the SECRET level and below. This policy includes any system/network with foreign/local national users. Release of DoD information shall be performed IAW DoD 5230.9 (Ref A-38).

h. Internet Connections. Component commands shall follow service policies on authorized use of the Internet. Prior to transmitting any information over a publicly accessible network (e.g., NIPRNET, Internet), or storing any information on a publicly accessible information system (e.g., a server connected to the NIPRNET), consideration shall be given to the releasability of the information to the general public or to the criticality of the information.

(1) These factors may warrant the use of additional security measures such as encryption or require prior clearance from a command Public Affairs Office, especially if the information is to be placed on a World Wide Web or otherwise released to the public. Procedures for clearing electronic copies of information must be in consonance with procedures in place for clearing "hard" copy information.

(2) Be consistent with other leadership responsibilities for public and internal communication. The decision whether or not to establish an organizational web information service is delegated to the local commander. The local commander may delegate this authority to lower levels, but shall ensure that all information placed on publicly accessible web information services is properly cleared and released through a Public Affairs Office (PAO) or an office authorized to act for the PAO. Local commanders or their designee shall ensure that appropriate instructions and regulations governing the clearance and release of information on web information services are published.

i. Information on the Internet. Personnel subject to USEUCOM command authority shall not post or otherwise publish any information on the World Wide Web or Internet that compromises national security or places USEUCOM personnel at risk IAW ASD Memorandum "Removal of Personally Identifying Information of DoD Personnel from Unclassified Web Sites", 28 Dec 01. This prohibition includes sensitive unclassified information (e.g., information marked FOUO), classified information, and Privacy Act information.

j. Maintenance. Maintenance on information systems used for processing classified data shall be performed by personnel who are cleared for the most sensitive data processed by the system. Foreign/Local national personnel shall not perform maintenance on information systems used for processing classified data unless specifically authorized by the DAA. If the maintenance personnel are not cleared for the most sensitive data processed, then:

(1) The information systems must be declassified prior to maintenance, per the sections of Appendix F dealing with remanence and disposal, or;

(2) The maintenance personnel must work under continuous supervision of cleared personnel who are knowledgeable of the system operations and who are able to control the access to information in the system.

k. Removable Media. All removable media shall be scanned for viruses prior to use in government information systems. If music CDs are allowed, PCs shall be configured to disable the autoplay feature, and CDs shall be virus checked prior to use.

l. Personal Electronic Devices (PEDs). PEDs include Personal Digital Assistants (PDAs), Handheld Computers, and data-enabled cell phones (hereafter collectively referred to as PEDs). All USEUCOM organizational commanders, HQ USEUCOM Staff Directorates, and separate offices shall ensure that PEDs and their internally stored data are protected IAW the requirements defined in this appendix. Security requirements shall be accomplished through protective features in the PED such as software design and configuration. Administrative, technical, physical and personal security controls shall be developed and all shall be documented in appropriate information system instructions and/or network user agreements. In HQ USEUCOM, PEDs are categorized as either Mission Support or Non-Mission Support. For the purposes of the policy, Mission Support PEDs are defined as those devices procured by a DoD Agency for official use. Non-Mission support are those devices that are personally owned and/or for personal use only. Both categories shall undergo appropriate accreditation prior to being synchronized with any operational network.

(1) Mission Support PEDs:

i. Mission support PEDs may be approved for operation at the classified or unclassified level as defined in the accreditation package.
ii. Mission support PEDs shall be fully integrated into the configuration management support infrastructure, to include organizational help-desk support.
iii. Mission support PEDs shall be safeguarded, managed and controlled to prevent disclosure of classified and/or sensitive information. .

(2) Non-Mission Support PEDs: Are privately owned for personal use PEDs to include contractor-supplied PEDs. The user shall assume full responsibility for non-mission support PEDs to include procurement, maintenance, repair, loss, and punitive liability should the loss involve compromise resulting from non-compliance with this appendix.

i. Non-mission support PEDs shall not be connected to any government equipment (classified or unclassified) including laptops, workstations, and peripherals.

ii. Non-mission support PEDs shall be prohibited from processing classified or sensitive-unclassified information.

iii. Non-mission support PEDs suspected of being contaminated with classified information shall be confiscated until a determination can be made regarding circumstances and device disposition. If contamination is confirmed the PED must be sanitized IAW regulations governing the sanitization of information systems storage devices. If the technology is not available for sanitization the PED shall be destroyed IAW with regulations governing the destruction of classified hardware.

iv. Non-mission support PEDs shall be clearly marked with user identification prior to being allowed in any official workspace.

m. Toner Cartridges. Drum type toner cartridges commonly used in standard laser jet printers, as well as multi-function printer/fax/copiers have the potential of retaining data on the cylinder heads after use. Prior to disposal of a cartridge used on a classified system as unclassified waste five pages with no margins of random alphanumeric characters shall be printed. Reference DCID 1/21 for further information.

n. User Logins

(1) If a userid and password control the access to an account on a system processing marked and protected information, then the userid and password combination is classified at the highest level encountered on that system (e.g. US SECRET NOFORN if the system processes up to U.S. SECRET NOFORN). Handling requirements for classified userid and password combinations are the same as for any other information of the same classification level.

(2) If a userid and password control access to an account on a system that processes unclassified information, the userid and passwords are considered Sensitive Information as defined by the Computer Security Act of 1987.

Note: Temporary waivers can be granted on a case-by-case basis for systems that do not currently have an encryption capability for Sensitive information. For systems where no encryption means is currently available, managers responsible for the system are required to inform all users of the danger of logging into that system, and are further responsible for notifying ECJ6-I of the lack of encryption capability and the steps being taken to provide such capability.

o. Remote Access via Modem. Remote access shall be allowed only with an appropriate level of authentication, encryption and physical protection to match the classification of the accessed information system. Access tables shall remain current. Call forwarding is prohibited when callback or dialback technology is used.

p. Software patches. Install vendor-produced system patches and implement procedural countermeasures according to DISA-EUR, DoD-CERT, or Service CERT guidance immediately upon receipt. In the rare case where security relevant system patches cannot be implemented, exceptions must be documented in the risk analysis.

q. Cell Phones. All commands shall develop a security policy for cell phones that addresses use of cell phones in areas where classified information is discussed. The policy shall consider the frequency of discussions, the sensitivity of the information discussed and the threats of the local environment.

r. Non-Government Information Systems. Use of non-government information systems for official government business is discouraged. Commands that allow the use of non-government information systems shall develop local policy governing their use. If the command provides web-accessible e-mail access (e.g. Outlook Web Access) then the command shall develop policy governing the use of the accessing information system. All use of non-government information systems shall be approved by the cognizant DAA. At a minimum, a local policy for the use of non-government information systems shall address the following:

(1) The determination to allow privately owned information system connections to government-information systems shall be made on a case-by-case basis by the cognizant system DAA. There shall be a standard agreement signed by anyone using a privately owned system for work-related purposes. It should state that signing the agreement constitutes consent to inspection, temporary possession, and the personal assumption of risk for any damages that may result from attempts to clear government-owned information from the personal property.

(2) The risk to government information.

(3) The possible loss-of-use of system resources or productivity if the system should become contaminated with Government Interest information, classified or unclassified.

(4) The procedures to be followed by the appropriate security official in the case of system contamination

i. How to report contamination
ii. Rules to be followed to preserve chain of evidence
iii. The recovery procedures to be followed
iv. How non-government files or media shall be protected and how access to these files, if not contaminated with Government Interest information, shall be provided to the owner in an expeditious manner.

s. Mobile Code. Mobile code technologies used within DoD have been categorized based on risk. Configuration guidance shall be provided by the Components and supporting elements IAW DoD Mobile Code Policy (Ref. A-4).

t. Encryption. All classified communications shall be secured using NSA-approved Type I encryption products. Components and supporting element shall develop policy and guidance addressing the safeguarding of FOUO communications. A specific risk analysis shall be performed for products that have not been formally approved by NSA. Reference NSTISSP No. 11, National Information Assurance Acquisition Policy.

(1) Transmission Security (TRANSEC): Bulk encryption (also known as link-by-link encryption) serves to nullify the ability of a cryptanalyst to identify important OPSEC indicators, such as sudden increases in traffic volume, when the increases are occurring, and (in many cases) who is talking to whom. The solution for eliminating or suppressing such OPSEC indicators is the responsibility of the network owners or, in the case of a tactical switching and transmission system, the local area commander. It is USEUCOM policy to include bulk encryption practices and methods in the accreditation process of networks and systems.

(2) It is recommended that Sensitive But Unclassified (a.k.a "Controlled Unclassified") information as well as Sensitive information as defined in the Computer Security Act of 1987 not be posted on nor transmitted over the Internet/ NIPRNET without appropriate NSA-approved products, techniques and/or protected services, or those that have been evaluated by NSA or an NSA-approved evaluation laboratory as being suitable for protection of sensitive information. Commands and supporting elements shall develop policy and guidance addressing safeguarding of SBU and Sensitive Unclassified information.

u. COMSEC/Information Systems Monitoring. All USEUCOM information systems and computer networks shall be monitored in accordance with Ref A-23 in order to detect, isolate, and react to intrusions, disclosures, disruption of services, or other incidents that threaten the security or function of DoD operations, DoD information systems, or computer networks. All forms of voice and data communications are subject to monitoring. Requests for COMSEC monitoring shall be submitted to ECJ6-I and coordinated for J3 approval through J39 for tasking to the Joint COMSEC Monitoring Activity (JCMA). COMSEC monitoring shall also be requested for all exercises directed by USEUCOM or led by a USEUCOM-directed JTF.

(1) COMSEC monitoring determines the amount of protection being provided to classified or sensitive information and, in so doing, provides a measure of force protection. In order to improve the theater COMSEC posture, results of COMSEC monitoring must be shared (at the operational level) among involved Components and supporting elements and organizations. When operating under HQ USEUCOM or JTF/CTF tasking, the JCMA shall be authorized to share life or mission-threatening information with organizations affected by the information revealed.

The legal restrictions associated with COMSEC monitoring require that information gathering be used only to improve overall operational security and not to punish individuals.

(2) Components and supporting elements shall certify to ECJ6-I their compliance with DoD Directive 4640.6 "notification and consent requirements" biennially in even numbered years, running from 1 October of the current even numbered year to 30 September two years following.

v. Incident Reporting **.** Timely and accurate incident reporting is critical to allow local, regional and global authorities to detect and respond to coordinated attacks. Commanders at all levels are responsible for establishing incident reporting procedures within their AOR, and are further responsible for establishing procedures to notify supporting intelligence and law enforcement organizations. Information assets include data, information-based processes, information systems, and information transfer links and mechanisms. An Information Event is any pre-assessed suspicious or anomalous activity affecting an information asset. An Information Incident is an assessed information event indicating an adversarial attack on an asset. At a minimum, all information events and incidents affecting USEUCOM information assets shall be reported using the procedures described below.

(1) Any user noticing anomalous or suspicious activity shall report the situation to their local network support activity (i.e. BNCC, NSC, NOSC, Help Desk). Users shall report events as they occur, or as they are recognized.

(2) Local network support activities noting an information event or incident shall issue a report to DISA's European Computer Emergency Response Team (EUR-CERT), the appropriate service CERT or CIRT, and supporting law enforcement and intelligence organizations in accordance with local procedures. Information events and incidents should be reported as they occur. Reports should be distributed in as timely a manner as is possible, even if the initial reports are brief. DISA-EUR EUR-CERT shall report this information to the TCCC IA Cell as soon as possible but at a minimum reports shall be provided within 4 hours of receipt of a report.

(3) Service CERTs and CIRTs detecting information events or incidents affecting USEUCOM assets shall report them to the affected local network support activity and EUR-CERT. The EUR-CERT shall report this information to the TCCC as soon as possible but at a minimum reporting shall be accomplished within 4 hours of receipt.

(4) Reports should be submitted based upon the most protected means for the affected system. Use SIPRNet or STU-III if those systems are available.

(5) EUR-CERT is responsible for gathering all event and incident reports for the USEUCOM AOR and performing analysis to generate and assess the status and welfare of the region's information environment. EUR-CERT shall report

information events and incidents in the CINC AOR to the CINC staff and local intelligence and law enforcement agencies in accordance with locally developed procedures. EUR-CERT shall also, in coordination with the USEUCOM ECJ3 and the TCCC, provide situational awareness information concerning incidents occurring in the USEUCOM AOR to elements within the AOR and lateral Regional Network Operations and Security Centers (RNOSCs).

(6) Information events or incident reports shall contain applicable classification markings and caveats (as determined by the applicable Security Classification Guidance), basic contact information, Minimum Essential Elements of Information (who, what, when, where, why and how), and the action taken. Security Classification Guidance shall be developed and disseminated through the DISA Global Network Operations and Security Center (GNOSC), and in the absence of specific guidance all reports shall be treated as For Official Use Only as a minimum.

w. Information Assurance Vulnerability Alert (IAVA) Reporting Process. Information Assurance Vulnerability Alerts (IAVA) are issued by the Commander, Joint Task Force, Computer Network Operations (JTF-CNO), in coordination with the Defense Information Systems Agency (DISA), and are pre-coordinated with the Service/Agency Computer Emergency response teams (CERTs)/Computer Incident Response Teams (CIRTs). HQ USEUCOM TCCC in conjunction with the EUR-CERT shall be the tasking authority for IAVAs within the EUCOM theater. Components and supporting elements shall implement EUCOM-directed IAVAs in accordance with EUCOM reporting requirements. In the event of conflicting direction between Service CERT/CIRTs and EUCOM-directed IAVAs, the EUCOM-directed IAVAs will have precedence. Components and supporting elements shall acknowledge IAVA receipt and report accomplishment of directed actions to the USEUCOM TCCC. Commanders at all levels are responsible for establishing IAVA implementation and reporting procedures within their AOR. Information Assets include data, information-based processes, information systems, and information transfer links and mechanisms. For more information on IAVA reporting, see Appendix M.

x. Information Operations Conditions (INFOCONS). DoD Directive 0-8530.1 assigns USCINCSPACE operational authority to direct Defense-wide changes in INFOCONS. USEUCOM shall direct changes to theater INFOCONS as required by the combination of threats, vulnerabilities, political and military conditions, and friendly operations. USEUCOM may direct specific measures to be taken with a change in INFOCON, or may direct that all applicable DoD level measures be taken. Components and supporting elements may declare a higher INFOCON level for their own component elements, and may enact additional measures, but any such changes or additions shall be immediately reported to the USEUCOM ETCC and HQ USEUCOM J39 IO Cell for purposes of informing lateral elements and the Joint Staff. Components and supporting elements shall implement EUCOM-directed INFOCONs in accordance with EUCOM reporting requirements. Prior to implementation, HQ EUCOM will coordinate the specified INFOCON change with components to ensure no adverse technical or operational impact. In the event of a variance between EUCOM and Service INFOCON Policy, Components and supporting elements will coordinate deconfliction between Service and EUCOM policy and/or report issues requiring assistance for resolution. In all cases, USCINCEUR guidance shall take precedence within the USEUCOM theater. INFOCON reporting requirements are provided in Appendix H.

y. Release of COMSEC Equipment to Foreign Allies. All USEUCOM Components and supporting elements and elements shall follow the procedures in Appendix I whenever they determine there is a requirement for releasing COMSEC information or equipment to a foreign government. Appendix I implements procedures to meet the requirements of CJCSI 6510.01C.

z. Protected Distribution Systems (PDS). PDS are used to transmit unencrypted classified National Security Information through an area of lesser classification or control. All PDS shall be designed, constructed and inspected to standards outlined in NSTISSI No. 7003, Protected Distribution Systems (PDS). All PDS designs shall be approved by component DAA and included in the system SSAA.

aa. Information Assurance Acquisition Policy. Information Assurance shall be considered as a requirement for all systems used to enter, process, store, display or transmit national security information (NSI). Effective 1 July 2002 the acquisition of all Commercial Off the Shelf (COTS) IA and IA-enabled Information Technology (IT) products to be used on systems processing NSI shall be limited only to those products which have been evaluated and validated by:

(1) The International Common Criteria for Information Security Technology Evaluation Mutual Recognition Arrangement;

(2) The National Security Agency (NSA)/National Institute of Standards and Technology (NIST) National Information Assurance Partnership (NIAP) Evaluation and Validation Program, or;

(3) The NIST Federal Information Processing Standard (FIPS) validation program. Guidance is contained in NSTISSP No. 11, National Information Assurance Acquisition Policy.

Appendix C

Information System Personnel Appointment and Training

C-1. **General.** This appendix describes the requirements for appointing and training information system personnel who are responsible for implementing and ensuring adherence to information assurance policy.

C-2 **Appointments.** All information system security positions shall be designated in a formal duty appointment specifying all duties and responsibilities, including the facilities, organizational elements, or information systems for which the appointed person is responsible. Commands will define other supporting positions (i.e., Remote Terminal Area Security Officer, ISSO Agent, Information Assurance Professionals, Work Group Administrator). A detailed description of all program manager positions and responsibilities can be found in Appendix A to Enclosure A to CJCSM 6510.01

C-3 **Training Requirements.** All persons appointed to one of the program management positions shall receive training in the proper execution of their job and Information Assurance responsibilities prior to commencing their duties. Commands will define documented training plan/programs to ensure proper training is completed. Commands will maintain documented training records of all information systems personnel. The Commands training will include at a minimum the following specific training/certification requirements:

a. User training: All users will receive initial security user training prior to gaining access and must be required to complete annual refresher training to maintain access to information systems.

b. SA training: All system administrators will be required to be able to pass level 1 certification to begin administration of information system and must pass level 2 certification within 1 year.

c. Security Officers: This includes all ISSOs, ISSMs, TASO or similar Information Assurance Professionals, must at a minimum attend a form of DITSCAP training and operations information systems security training, such as INFOSEC 301 and 315 training provided by DISA.

Appendix D

Accreditation

D-1. **General.** Designated Approval Authorities (DAAs) in USEUCOM are responsible for certification and accreditation of each system and network under their jurisdiction. Certification and accreditation shall be accomplished in accordance with DoD Directive 5200.28, DoD Instruction 5200.40, and DoD Information Technology Security Certification and Accreditation Process (DITSCAP) dated 30 Dec 97.

a. All test-bed or demonstration systems require security approval from the cognizant DAA before connection to any approved network or before processing any classified or sensitive information.

D-2. **Memorandum of Agreement (MOA)**: When information systems managed by different DAAs are interfaced or networked, an MOA is required that addresses the accreditation requirements for each information system involved.

D-3. **DISN Connections**. All information system connections to the DISN shall comply with the applicable DISN Connection Approval Process (DISN Connection Security Requirements, Nov 1997).

D-4. **SABI/TSABI.** All system interconnections which pass information between systems operating at different security levels shall comply with the SABI/TSABI process IAW OASD/C3I Policy Memorandum “SABI Reaffirmation”, 11 May 98.

Appendix E

Markings

E-1. **General.** Executive Order 12958 prescribes a uniform system for classifying, safeguarding, and declassifying national security information. The order states that classified documents "shall, by marking or other means, indicate which portions are classified, with the applicable classification level, which portions are exempt from declassification . . . and which portions are unclassified." Complying with the requirements of the order requires the labeling of information residing in electronic classified information systems. At a minimum, "all electronic classified information in the form of documents, images, or other human-viewable formats shall require plain-text markings indicating classification, handling restrictions, classifying authority, and declassification instructions, as would be required if they were paper products." New databases or other similar data repositories shall include database columns for identifying plain-text labels, or equivalent methods for labeling data elements.

E-2. **System Identification Screen.** All computer display monitors shall display a system identification screen prior to allowing any logon. This screen shall include the following information:

a. The security classification level of the system, essential control markings and compartments (e.g., UNCLASSIFIED, SECRET REL NATO, TOP SECRET). This requirement is optional for unclassified systems and networks that are not intended for use in an area where classified information is processed.

b. The name of the proponent organization for the system or network (e.g., HQ U.S. European Command; U.S. Army 5th Signal Command). The name may be displayed within an organizational logo, if the name is complete and legible.

c. The name of the system or network (e.g., Global Command and Control System; HQ USEUCOM SECRET LAN)

d. The DoD Logon Warning Banner. All information systems must display a DoD-approved logon-warning banner. Service commands may use a warning banner approved by their service. The banner must be included in the system identification screen. If the banner does not fit in this screen, it must be displayed in an alternative manner as prescribed by DoD policy or service policy. Personnel must not be permitted to log in without agreeing to the login banner.

E-3. **Softcopy documents.**

a. Softcopy implies all documents in electronic form and includes but is not limited to: e-mail, memos, charts, and web pages/files. This includes documents in any state of completion, including official and draft documents.

b. Minimum requirements within USEUCOM shall include individual paragraph or portion makings; classification at top and bottom of pages or at top and bottom of web file, and "Derived by / declassify on" markings on all softcopy documents.

c. All markings shall allow a user to quickly and continuously be aware of the classification of the document / web page or file.

d. All information to be published on a web page shall be reviewed with the "Need-to-Release" principle in mind. Carefully consider whether the information should be made widely available.

e. All web pages shall be classified based on their individual content, regardless of the classification of the pages to which they link.

E-4. **E-mail.** All commands shall develop a methodology for quickly identifying the classification of e-mail. All e-mail, both classified and unclassified will begin with a banner stating the classification of the e-mail. Unclassified e-mail with classified attachments marked as classified, are marked with a second banner stating "UNCLASSIFIED WHEN CLASSIFIED ATTACHMENTS REMOVED". Classified e-mail with classified attachments also contains a second banner when the classification of the e-mail is lesser than the classification of the attachment, for example "DOWNGRADE TO CONFIDENTIAL WHEN UNCLASSIFIED ATTACHMENTS REMOVED". Further guidance on how to apply markings can be found in DoD 5200.1-PH.

Appendix F

Media Reuse

F-1. **General.**

a. There are two means of destroying data on magnetic media: overwriting and degaussing.

(1). *Overwriting* destroys data on storage media by recording patterns of unclassified data over the data stored on the media.

(2). *Degaussing* (also known as demagnetizing) reduces magnetic induction to zero by applying a reverse magnetizing field.

b. The Department of Defense requires the use of DoD 5200.28-M by DoD components, but heads of DoD components may augment these requirements to meet their needs by prescribing more detailed guidelines and instructions provided they are consistent with these policies. Ultimately, the Information Systems Security Manager (ISSM) is responsible for the security of all information systems and media assigned to the organization and under their purview. To protect these assets, ISSMs must ensure that the applicable DoD and service security measures and policies are followed.

c. Users wishing to downgrade, declassify or release media are to contact their governing ISSO, who shall make decisions and prescribe procedures based on the applicable DoD and service regulations.

F-2. **Equipment Disposal.** Commands shall ensure that information systems and computer storage media which have been used for processing classified information or sensitive unclassified information are appropriately erased, declassified or destroyed prior to transfer to a DoD supply system, the DRMO, an entity outside DoD, or trash bins. Commands shall follow DoD guidelines as published in the Assistant Secretary of Defense Memorandum, 8 Jan 2001, 29 May 2001 and 4 Jun 2001 for sanitizing and releasing equipment. No previously classified magnetic media shall be disposed of via DRMO.

Appendix G

Deployed Information Assurance

G-1. **General.** Commands must have flexible, realistic deployment plans to ensure that Information Assurance is factored into all traditional and non-traditional peacetime, contingency, combat, or coalition operations. The deployment plans must cover every system subject to deployment or connectivity to a deployed location. Command DAAs shall specify in the system security accreditation letter that a system can be deployed and operated in accordance with the deployment plans. Deployment plans shall address the following security points:

a. The persons or offices authorized to order deployment of the system.

b. Additional security approvals required for deployment and the office responsible for obtaining them.

c. Requirements for deployed ISSOs. All deployment plans with requirements for deployed ISSOs shall ensure that ISSOs have received proper training, prior to deployment, in related disciplines. This training should include, but is not limited to: Network Security Officer, Security Life Cycle Manager, System Administrator, and Configuration Manager. Such training is needed to ensure that deployed ISSOs are prepared to handle any situation they may encounter.

d. Secure transport of the system to the deployment site, and secure return transport to garrison.

e. Physical security of the system at the deployment site.

f. System configuration changes required for deployment.

g. COMSEC and Protected Wireline Distribution System (PDS) requirements at the deployment site.

h. Secure installation and maintenance at the deployment site. IA devices shall be deployed and implemented IAW Appendix B for enclave protection in a deployed environment. If expertise is not available in the deployed location, the IA devices may be remotely administered by the command Network and Operations Security Center (NOSC). Verification of the security clearances of new users at the deployment site, and essential user security training.

j. Emergency destruction plans for the deployment site.

k. Plans for restoration / reconstitution of the system and infrastructure.

l. Multinational/coalition-networking considerations.

G-2 **COMSEC for deployments.** Commanders are responsible for ensuring the security of information transmitted over their communications systems and media. At a minimum, commanders shall consider:

a. Availability of appropriate COMSEC equipment and keying material (Note: It is HQ USEUCOM policy that COMSEC for deployments be generated as closely as possible to the time of need and in direct response to the particular network requirements. See Appendix K for detailed guidance.)

b. Personnel training in use of COMSEC equipment and over-the-air key distribution operations. Specific attention shall be given to the accountability and protection of key storage and fill devices; e.g., the AN/CYZ-10 Data Transfer Device and future versions thereof.

c. Requirements for release of COMSEC devices to foreign/local nationals for interoperability, as stated in CJCSI 6510.01C.

G-3. **Travel.** Commands shall ensure that all persons are aware of and have had training in proper information system security procedures and their information assurance responsibilities to ensure proper protection of information and information systems while traveling. This training should also include procedures for reporting possible security incidents, required use of encryption systems, and other IA measures. Special consideration should be given to travel in high risk areas; consult your local force protection office.

Appendix H

Information Operations Conditions (INFOCONS)

H-1**. General.** This appendix provides guidance to USEUCOM components for implementing Information Operations Condition (INFOCON) levels. It pertains to all information and telecommunication systems operating at the SECRET and below level. Guidance provided herein is to be considered both a directive and an authorization for USEUCOM operational commanders to increase the readiness of information systems and networks under their purview. The USEUCOM INFOCONS are applicable to all USEUCOM forces, including Component Commands, Subordinate Unified Commands, and Joint Task Forces (JTF). Components and supporting elements shall implement EUCOM-directed INFOCONs in accordance with EUCOM reporting requirements. Prior to implementation, HQ EUCOM will coordinate the specified INFOCON change with components to ensure no adverse technical or operational impact. In the event of a variance between EUCOM and Service INFOCON Policy, Components and supporting elements will coordinate deconfliction between Service and EUCOM policy and/or report issues requiring assistance for resolution. In all cases, USCINCEUR guidance shall take precedence within the USEUCOM theater.

H-2**. Responsibilities.**

a. HQ USEUCOM, Operations Directorate, ECJ3: By authority of the CINCEUR, EUCOM Chief of Operations, ECJ3, will declare changes to EUCOM INFOCON levels.

(1) HQ USEUCOM, Information Operations Directorate, ECJ39:

(a) Under the Authority of the J3, the ECJ39, Information Operations Directorate will act as staff lead for INFOCONs. The Computer Network Defense Information Operations Cell (CND IO Cell) and the Information Operations Working Group (IOWG) are used to assess the operational impact of an INFOCON change.

(b) The members of the IO CND Cell will consist of action officers from ECJ22-TI, ECJ6-I, ECJ6-TCCC, DISA-EUR, ECJ39-O, and ECPA. The CND IO Cell will be chaired by the J39. This group will serve as the immediate (less than one hour) EUCOM assessment to an impending INFOCON change. ECJ39, through the CND IO Cell and the TCCC, will:

(1) Coordinate directly with supporting CINCs and USCINCSPACE to resolve reporting-requirement conflicts at the joint-theater level.

(2) Coordinate and review threat information, network activity, other CINC activity and operational impact, and provide INFOCON change recommendations to IOWG.

(3) Take the recommendations from the CND IO Cell and forward the recommendation to the ECJ3 for approval.

(4) When time permits, convene the IOWG to review the CND IO Cell assessment for further analysis. The members of the IOWG will consist of senior leaders from ECJ22-TI, ECJ6-I, ECJ6-TCCC, DISA-EUR, ECJ39-O, and ECPA.

b. HQ USEUCOM, Communications Directorate, ECJ6:

(1) HQ USEUCOM, Information Assurance (IA) Division, ECJ6-I:

(a). Provide policy guidance and J6 representation to the HQ EUCOM Information Operations Working Group (IOWG/J39).

(b). Coordinate with the HQ USEUCOM, J5 Plans and Policy Directorate to ensure INFOCON actions are integrated into the Deliberate Planning process to include NATO and Coalition interoperability requirements.

(c). Through supporting Network Operations and Security Centers (NOSCs), coordinate release and sharing of INFOCON changes with affected customers.

(d). Review all network-related activities for potential impact upon USCINCEUR operations.

(2) HQ USEUCOM, Theater C4I Coordination Center, ECJ6-TCCC:

(a) Coordinate INFOCON changes with JTF-CNO and EUCOM theater Component commands.

(b) Maintain status and visibility of security posture of USEUCOM Networks.

(c) Coordinates all other IA matters throughout the theater.

c. HQ USAREUR, HQ NAVEUR, HQ USAFE, HQ MARFOREUR, and HQ SOCEUR:

(1). Review all network-related activities for potential impact upon USCINCEUR operations.

(2). De-conflict Service/agency reporting requirements as necessary to ensure INFOCON reporting complies with guidance provided herein.

d. DISA Europe

(1). Gather and analyze all network-related activities for potential impact upon USCINCEUR operations.

(2). Through the EURCERT, serve as the theater focal point for all network incident and event reporting.

(3). In coordination with the TCCC, provide situational awareness information concerning incidents occurring in the USEUCOM AOR, to elements within the AOR and lateral NOSCs.

H-3. **INFOCON Levels.** The INFOCON system is characterized by five progressive defensive postures. INFOCON levels are NORMAL, ALPHA (Low Activity), BRAVO (Significant Activity), CHARLIE (Serious Activity), and DELTA (Critical Activity). INFOCON levels are analogous to DEFCON, WATCHCON, and THREATCON levels but can vary in their application. Although events that would raise or lower those levels may directly affect the existing INFOCON level, USEUCOM could declare a higher or lower INFOCON level without the declaration of a similar DEFCON, WATCHCON, or THREATCON level change. These defensive postures are designed to support information operations throughout all levels of conflict.

H-4. **INFOCON Response Measures.**

a. USEUCOM specific response measures are listed in Annex A to this appendix.

b. Establishing an INFOCON does not presuppose specific response measures are activated. Upon declaration of an INFOCON level, HQ USEUCOM will direct specific defensive measures for implementation within the theater. Component, Subordinate Unified, JTF, and local commanders may not direct a lower INFOCON level than that set by HQ USEUCOM.

c. HQ USEUCOM directed measures do not preclude Component, Subordinate Unified, JTF, or local Commanders from initiating more restrictive measures, if desired, after notifying USEUCOM. Component, Subordinate Unified, JTF, and local commanders must first gain approval from HQ USEUCOM prior to directing their units to not implement specific desired response measures.

d. Component, Subordinate Unified, and JTF Commanders who receive conflicting INFOCON guidance from another Unified Command or Service will inform HQ USEUCOM J39. Within the USEUCOM AOR, USCINCEUR INFOCONs take precedence. Prior to implementation, HQ EUCOM will coordinate the specified INFOCON change with components to ensure no adverse technical or operational impact. In all cases, USCINCEUR guidance shall take precedence within the USEUCOM theater.

e. INFOCON response measures may be directed for implementation within a specific sub region within the USEUCOM AOR, or theater-wide depending on the actual situation.

f. INFOCON measures are not all inclusive. Each component, subordinate Unified, and JTF Commands will review these measures and develop supplemental INFOCON procedures as required.

H-5**. Reporting Procedures (DoD level INFOCON Changes).** By authority of the SECDEF, USCINCSPACE will declare changes to global DoD INFOCON levels. The following sequence of events will take place prior to a change declaration:

a. JTF-CND will coordinate with the C/S/As to determine the operational impact of changing the DoD INFOCON level. EUCOM TCCC will be the focal point for coordination with ECJ39 and JTF-CNO.

b. Based upon C/S/A inputs, the Commander, JTF-CNO will recommend changes in the DoD INFOCON to USCINCSPACE.

c. Upon receiving the recommendation from JTF-CNO, USCINCSPACE will assess, and if necessary, authorize a DoD-level INFOCON change. This change will be transmitted in the form of a General text message to all operations and networks centers. The General text message may be supplemented by a telephonic conference convened by USCINCSPACE or a designated representative.

H-6. **EUCOM INFOCON Change Message.** Once a DOD level INFOCON change is received, the EUCOM Theater Command Center (ETCC) notifies the CND IO Cell. The CND IO Cell lead, ECJ39, will convene the CND IO Cell and begin to evaluate threat information, network activity, operational impact and other CINC activity. TCCC, a member of the IO CND Cell, will coordinate with component operations centers/NOSCs and provide INFOCON change recommendations to CND IO Cell. CND IO Cell will review all current information, and if appropriate draft an INFOCON change message using the format in Figure H-1. If needed, CND IO Cell will forward the INFOCON message to the ECJ3 for approval. Once approved, the INFOCON message will be released to all EUCOM components from ECJ3 by the ETCC.

FIGURE H-1
USEUCOM INFOCON Change Message

UNCLASSIFIED

(Note that the information presented in this message is notional and is for example purposes only. Paragraphs marked as classified do not contain actual classified information.)

FM HQ USEUCOM VAIHINGEN GE//ECJ3//

TO CINCUSNAVEUR LONDON UK//00/01/019/N2/N3/N4/CDO//

CINCUSNAVEUR LONDON UK//N1/N5/N6/N7/013/018022//

HQ USAFE RAMSTEIN AB GE//CC/CV/DO/LG/SC/SCN//

USAFE AOS COMMAND POST RAMSTEIN AB GE//

HQ USAREUR HEIDELBERG GE//AEACC/AEAGC-O/AEAGD//

HQ USAREUR HEIDELBERG GE//AEAGC/AEAGB/AEAIM//

COMMARFOREUR

COMSOCEUR VAIHINGEN GE//J2/J3/J4/J6//

JAC MOLESWORTH RAF MOLESWORTH UK//CC/DO/DOI/DOO/DOT//

JAC MOLESWORTH RAF MOLESWORTH UK//SSO/ISSM/DOO/DSTS//

ODC ANKARA TU

ODC BONN GE

DISA EUR VAIHINGEN GE

INFO CJTF-CND WASHINGTON DC//J2/J3/JTF CND WO//

JOINT STAFF WASHINGTON DC//DJS/JSJ3/JSJ3-JOD/J39/J6//

JOINT STAFF WASHINGTON DC//JSJ2/JSJ2T/JSJ3-SOD//

HQ USEUCOM VAIHINGEN GE ECJ2/ECJ3/ECJ4/ECJ5/ECJ6//

HQ USEUCOM VAIHINGEN GE //ECJ1/ECJ33/ECJ35/J39/ECJ22T//

HQ USEUCOM VAIHINGEN GE //ETCC/ECPA/ECSO/ECLA/ECCM//

HQ USEUCOM VAIHINGEN GE//TCCC//

AIG 996 (All ODCs)

UNCLASSIFIED

SUBJ:EUCOM INFORMATION OPERATIONS CONDITION (INFOCON) CHANGE TO ALPHA (U)

REF/A/RMG/ JTF CNO /999999Z JAN 02/-/NOTAL//
REF/B/DOC/EUCOM 25-5/01MAR99//
NARR/REF A IS JTF CNO MESSAGE DIRECTING INFOCON CHANGE TO ALPHA DOD-WIDE. REF B, EUCOM INFORMATION ASSURANCE DIRECTIVE ED 25-5//
POC/TCCC/VARIOUS/TEL: DSN 314-430-4581, COMM: 49-0711-680-4581//
RMKS/1. (U) REF A DIRECTS DOD-WIDE INFOCON CHANGE TO ALPHA.
2. (U) IN LIGHT OF REF A ALL COMPONENTS, SUBORDINATE UNIFIED COMMANDS, AND JOINT TASK FORCES ARE HEREBY DIRECTED TO GO TO

INFOCON ALPHA IMMEDIATELY.
3. (U) ALL UNITS ACKNOWLEDGE RECEIPT OF THIS MESSAGE IMMEDIATELY TO EUCOM POC.
4. (U) EUCOM MEASURES TO ATTAIN INFOCON ALPHA APPLY TO BOTH SIPRNET AND NIPRNET AND ARE SPECIFIED IN ED 25-5 AND OUTLINED BELOW:
4A. (FOUO) MEASURE 1: VERIFY USEUCOM IO POINT OF CONTACT LIST OF PHONE NUMBERS, E-MAIL ADDRESSES, AND OFFICIAL MESSAGE TRAFFIC ADDRESS LIST.
4B. (FOUO) MEASURE 2: ALERT INTELLIGENCE COMMUNITY TO MONITOR THREAT FOR ADDITIONAL DIO INDICATIONS AND WARNINGS (I&W), AND INCREASED FOREIGN INTELLIGENCE AND INFORMATION ACTIVITY. ECJ2 TO NOTIFY NATIONAL INTELLIGENCE AGENCIES OF SAME, AND REQUEST INCREASED VIGILANCE AND REPORTING FROM THEM.
4C. (FOUO) MEASURE 3: ISSUE STATUS REPORT OF DIO ACTIVITIES TO THE USEUCOM TCCC AS DIRECTED IN THE INFOCON CHANGE MESSAGE IN ACCORDANCE WITH REPORT FORMAT
4D. (FOUO) MEASURE 4: ENSURE ALL COMMANDERS, SECURITY MANAGERS, INFORMATION SYSTEM SECURITY MANAGERS (ISSM), INFORMATION SYSTEM SECURITY OFFICERS (ISSO), SYSTEM ADMINISTRATORS (SA), COMSEC CUSTODIANS, AND OTHER COMMUNICATIONS OR INFORMATION SYSTEMS ORGANIZATIONS OR PERSONNEL ARE BRIEFED ON THE THREAT IO ACTIVITY, INFOCONS CHANGES, AND RESPONSE MEASURES.
4E. (FOUO) MEASURE 5: INCREASE OPSEC AWARENESS. INCLUDE THINGS SUCH AS REMINDING ALL USERS OF THE RISKS OF BEING MONITORED BY ADVERSARIES DURING E-MAIL AND PHONE USE.
5. (U) REPORT STATUS/ATTAINMENT OF INFOCON ALPHA WITHIN 24 HOURS TO EUCOM POC.
6. (S) IN THOSE CASES WHERE COMPONENT COMMANDERS FEEL IT IS APPROPRIATE TO INCREASE THE INFOCON ABOVE ALPHA OR TO TAKE ADDITIONAL INFOCON MEASURES, REPORT CHANGES, DIFFERENCES OR ADDITIONS TO EUCOM POC.
7. (U) EUCOM POC INFORMATION:

(Note that the information presented in this message is notional and is for example purposes only. Paragraphs marked as classified do not contain actual classified information.)

UNCLASSIFIED

H-7. **Acknowledgment.** Upon receipt of a USCINCSPACE INFOCON Change Declaration, the HQ EUCOM CND IO Cell, through the TCCC, will commence to poll the Service/agency-component Operations Centers listed in below subparagraphs via telephone or e-mail. During the poll, Operations Centers will be requested to acknowledge receipt, confirm that subordinate organizations are being notified, estimate time of completion for notifications, and declare any extenuating circumstances that may delay notification. The CND IO Cell, through the TCCC, will draft a message that acknowledges USCINCSPACE message using the Example HQ USEUCOM Acknowledgment Message (Fig H-2).

a. USAREUR
Operations Center DSN 314-377-4906
AUTODIN PLA: HQ USAREUR HEIDELBERG GE//AEACC/
AEAGC-O/AEAGD/AEAGC/AEAGB/AEAIM//
NIPR E-mail: u7a-cc@dcsops.hqusareur.army.mil
SIPR E-mail: u7a-cc@dcsops.hqusareur.army.smil.mil

b. (1) USAFE Network Operations and Security Center
DSN 314-480-7161
AUTODIN: USAFE NOSC RAMSTEIN AB GE//
DMS: USAFE NOSC (NIPR & SIPR)
(2) USAFE AOS Command Post
DSN 314-480-8200
AUTODIN: USAFE AOS COMMAND POST RAMSTEIN AB GE//
DMS: USAFE AOS COMMAND POST (NIPR & SIPR)
NIPR E-mail: USAFE.NOSC@RAMSTEIN.AF.MIL
SIPR E-mail: USAFE.NOSC@RAMSTEIN.AF.SMIL.MIL

c. USNAVEUR
Operations Center CDO
DSN: 314-235-4080
AUTODIN: CINCUSNAVEUR LONDON UK//CDO/N6/N64//
DMS: CINCUSNAVEUR LONDON UK (NIPR & SIPR)
NIPR E-mail: CNECDO@NAVEUR.NAVY.MIL;
CNEN64@NAVEUR.NAVY.MIL; CNEN642@NAVEUR.NAVY.MIL
SIPR E-mail: CNECDO@NAVEUR.NAVY.SMIL.MIL;
CNEN64@NAVEUR.NAVY.SMIL.MIL; CNEN642@NAVEUR.NAVY.SMIL.MIL

d. MARFOREUR
(1) Crisis Action Center
DSN (STU-III): 314-431-2380/2265
AUTODIN: COMMARFOREUR//
DMS: COMMARFOREUR
NIPR E-mail: MFEwatch@MFE.USMC.MIL
SIPR E-mail: MFEwatch@MFE.USMC.SMIL.MIL
(2) Network Operations Center
DSN: 314-431-2397
NIPR E-mail: MFEG6NOC@MFE.USMC.MIL
SIPR E-mail: MFEG6NOC@MFE.USMC.SMIL.MIL

e. DISA Europe

Regional Network Operations and Security Center
DSN 314-430-6372
AUTODIN: DISA EUR VAIHINGEN GE//EUA/EU3//
DMS: RNOSC-EUR
NIPR E-mail: RNOSC-EUR@EUR.DISA.MIL
SIPR E-mail: RNOSC-EUR@EUR.DISA.SMIL.MIL

f. Joint Analysis Center
Operations Center
DSN: 314-268-2367
AUTODIN: JAC MOLESWORTH UK//SSO/ISSM/DOO/DSTS//
SIPR E-mail: jocwatch@jac.eucom.smil.mil

Figure H-2

Example HQ USEUCOM Acknowledgment Message

UNCLASSIFIED

(Note that the information presented in this message is notional and is for example purposes only. Paragraphs marked as classified do not contain actual classified information.)

FM HQ USEUCOM VAIHINGEN GE//ECJ3//

TO USCINCSPACE PETERSON AFB CO//CC/J6/J2/J3/SPOC WO/J39//

CJTF-CND WASHINGTON DC//J2/J3/JTFCNDWO//

INFO JOINT STAFF WASHINGTON DC//NMCC//

CINCUSNAVEUR LONDON UK//00/01/019/N2/N3/N4/CDO//

CINCUSNAVEUR LONDON UK//N1/N5/N6/N7/013/018022//

HQ USAFE RAMSTEIN AB GE//CC/CV/DO/LG/SC/SCN//

USAFE AOS COMMAND POST RAMSTEIN AB GE//

HQ USAREUR HEIDELBERG GE//AEACC/AEAGC-O/AEAGD//

HQ USAREUR HEIDELBERG GE//AEAGC/AEAGB/AEAIM//

COMMARFOREUR

COMSOCEUR VAIHINGEN GE//J2/J3/J4/J6//

JAC MOLESWORTH RAF MOLESWORTH UK//CC/DO/DOI/DOO/DOT//

JAC MOLESWORTH RAF MOLESWORTH UK//SSO/ISSM/DOO/DSTS//

ODC ANKARA TU

ODC BONN GE

INFO AIG 996 (All ODCs)

DISA EUR VAIHINGEN GE

NCEUR VAIHINGEN GE//F29//

UNCLAS

SUBJ/(U)USEUCOM ACKNOWLEDGEMENT OF DOD INFOCON CHANGE (U)//
REF/A/MSG/ USCINCSPACE/DOD INFORMATION OPERATIONS CONDITION (INFOCON) CHANGE TO ALPHA/999999Z XXX 00//
GENTEXT/GENERAL/1.(U) HQ USEUCOM ACKNOWLEDGES RECEIPT OF USCINCSPACE MESSAGE, SUBJ: DOD INFORMATION OPERATIONS CONDITION (INFOCON) CHANGE TO ALPHA, DTG 999999Z XXX 00. EUCOM TCCC IS NOTIFYING ALL SUBORDINATE UNITS. EUCOM TCCC WILL PROVIDE USSPACECOM/JTF-CNO UPDATE ON INFOCON NOTIFICATION AND IMPLEMENTATION STATUS VIA CND INFOCON SITREP NLT 999999Z XXX 00.

2.(U) POC INFORMATION. EUCOM THEATER COMMAND CENTER WATCH OFFICER, DSN: XXX-XXX-XXXX, NIPRNET: XXXX.HQ.DLA.MIL.//

(Note that the information presented in this message is notional and is for example purposes only. Paragraphs marked as classified do not contain actual classified information.)

UNCLASSIFIED

H-8. **Component Acknowledgement Reporting.** All component command centers will acknowledge receipt of the EUCOM message directing change in INFOCON level to the ETCC using the format in Figure H-3.

Figure H-3
Example Component Acknowledgement Message

UNCLASSIFIED

(Note that the information presented in this message is notional and is for example purposes only. Paragraphs marked as classified do not contain actual classified information.)

FM ***REPORTING COMPONENT***

TO HQ USEUCOM VAIHINGEN GE//ECJ3/TCCC//

INFO DISA EUR VAIHINGEN GE//   //

HQ USEUCOM VAIHINGEN GE//ECJ6-I/ECJ6-O//

NCEUR VAIHINGEN GE//F29//

U N C L A S

SUBJ/(U)ACKNOWLEDGEMENT OF EUCOM INFOCON CHANGE (U)//
REF/A/MSG/ USCINCEUR INFORMATION OPERATIONS CONDITION (INFOCON) CHANGE TO ALPHA/999999Z XXX 00//
GENTEXT/GENERAL/1.(U) HQ ***REPORTING COMPONENT*** ACKNOWLEDGES RECEIPT OF USCINCEUR MESSAGE, SUBJ: EUCOM INFORMATION OPERATIONS CONDITION (INFOCON) CHANGE TO ALPHA, DTG 999999Z XXX 00. ***REPORTING COMPONENT*** IS NOTIFYING ALL SUBORDINATE UNITS. WE WILL PROVIDE USEUCOM UPDATE ON INFOCON NOTIFICATION AND IMPLEMENTATION STATUS VIA CND INFOCON SITREP NLT 999999Z XXX 00.

2.(U) POC INFORMATION. EUCOM THEATER COMMAND CENTER WATCH OFFICER, DSN: XXX-XXX-XXXX, NIPRNET: XXXX.HQ.DLA.MIL.//

(Note that the information presented in this message is notional and is for example purposes only. Paragraphs marked as classified do not contain actual classified information.)

UNCLASSIFIED

H-9**. Compliance Status Reporting.** The CND IO Cell, through the TCCC, will monitor current status of all Service/Agency components until the INFOCON change has been achieved and/or exceptions are accounted for. The TCCC Watch Officer will ascertain the following:

a. Situation and status of networks for each CND directive measure established by USCINCSPACE as well as any additional measures directed by HQ USEUCOM.

b. Estimated time of completion for achieving compliance, or for accounting for exceptions to implementation measures.

c. Operational impacts associated with implementation.

d. Additional CND measures directed at the Service/Agency component level.

e. Any assigned INFOCON levels other than the DoD level. (Include level and estimated time of attainment or reason for non-attainment)

f. Service/Agency components will report INFOCON compliance status as directed in the INFOCON change message, and as changes in status occur. Compliance status will be reported using the message format in Figure H-4.

Figure H-4

Component Compliance SITREP

UNCLASSIFIED

(Note that the information presented in this message is notional and is for example purposes only. Paragraphs marked as classified do not contain actual classified information.)

FM (*REPORTING COMPONENT*)

TO HQ USEUCOM VAIHINGEN GE//ECJ6/TCCC//

INFO CINCUSNAVEUR LONDON UK//00/01/019/N2/N3/N4/CDO//

CINCUSNAVEUR LONDON UK//N1/N5/N6/N7/013/018022//

HQ USAFE RAMSTEIN AB GE//CC/CV/DO/LG/SC/SCN//

USAFE AOS COMMAND POST RAMSTEIN AB GE//

HQ USAREUR HEIDELBERG GE//AEACC/AEAGC-O/AEAGD//

HQ USAREUR HEIDELBERG GE//AEAGC/AEAGB/AEAIM//

COMMARFOREUR

COMSOCEUR VAIHINGEN GE//J2/J3/J4/J6//

JAC MOLESWORTH RAF MOLESWORTH UK//CC/DO/DOI/DOO/DOT//

JAC MOLESWORTH RAF MOLESWORTH UK//SSO/ISSM/DOO/DSTS//

ODC ANKARA TU

ODC BONN GE

DISA EUR VAIHINGEN GE

HQ USEUCOM VAIHINGEN GE//ECJ6-I/ECJ6-O//

NCEUR VAIHINGEN GE//F29//

INFO AIG 996 (All ODCs)

SECRET

MSGID/SITREP/USCINCEUR//

SUBJ/SITREP/USEUCOM COMPUTER NETWORK DEFENSE (CND) SITREP(U)//

REF/A/MSG/USCINCSPACE/DOD INFORMATION OPERATIONS CONDITION (INFOCON) CHANGE TO ALPHA/999999Z JAN 02//
REF/B/MSG/USCINCEUR/INFORMATION OPERATIONS CONDITION (INFOCON) CHANGE TO ALPHA/999999Z JAN 02//

GENTEXT/GENERAL/
NARR/REF A IS USCINCSPACE MESSAGE DECLARING DOD INFOCON CHANGE.//REF B IS USCINCEUR MESSAGE DECLARING EUCOM INFOCON CHANGE WITH DIRECTIVE MEASURES.//
RMKS/1.(S) SITUATION/DISPOSITION/STATUS OF FORCES. (***REPORTING COMPONENT***) INFORMATION NETWORKS ARE FULLY OPERATIONAL. ALL FORCES IMPLEMENTING USCINCEUR-DIRECTED INFOCON ALPHA, EFFECTIVE 999999Z JAN 02. EXCEPTION IS 414TH SIGNAL COMPANY WHICH REMAINS AT INFOCON BRAVO DUE TO SUSPECTED INTRUSIONS INTO DEPLOYED TRI-TAC NETWORK.

2.(U) OPERATIONS.
2.A.(U) INFOCON DIRECTED MEASURE COMPLIANCE STATUS.
(U) EUCOM MEASURE 1
(U) COMPLIANCE STATUS: ALL UNITS REPORT FULLY COMPLIANT
(U) ESTIMATED TIME TO COMPLETION: N/A
(U) LIMITING FACTORS: N/A

(U) EUCOM MEASURE 2
(U) COMPLIANCE STATUS: ALL UNITS REPORT FULLY COMPLIANT
(U) ESTIMATED TIME TO COMPLETION: N/A
(U) LIMITING FACTORS: N/A

(U) EUCOM MEASURE 3
(U) COMPLIANCE STATUS: ALL UNITS REPORT FULLY COMPLIANT
(U) ESTIMATED TIME TO COMPLETION: N/A
(U) LIMITING FACTORS: N/A

(U) EUCOM MEASURE 4
(U) COMPLIANCE STATUS: ALL UNITS REPORT FULLY COMPLIANT
(U) ESTIMATED TIME TO COMPLETION: N/A
(U) LIMITING FACTORS: N/A

(U) EUCOM MEASURE 5

(U) COMPLIANCE STATUS: ALL UNITS REPORT FULLY COMPLIANT
(U) ESTIMATED TIME TO COMPLETION: N/A
(FOUO) LIMITING FACTORS: CONTRACT LIMITATIONS CURRENTLY RESTRICT SYSTEM ADMINISTRATOR OVERTIME HOURS FOR SEVERAL PACOM UNITS. THESE UNITS ARE INCREASING AUDITS WHILE STAYING WITHIN CONTRACT REQUIREMENTS.

(U) EUCOM MEASURE 6
(U) COMPLIANCE STATUS: ALL UNITS REPORT FULLY COMPLIANT
(U) ESTIMATED TIME TO COMPLETION: N/A
(U) LIMITING FACTORS: N/A

(U) EUCOM MEASURE 7
(S) COMPLIANCE STATUS: ALL EUCOM GCCS SYSTEMS NON-COMPLIANT
(U) ESTIMATED TIME TO COMPLETION: UNK. PENDING GCCS VALIDATED PATCH TO IAVA 2000-A-0002.
(U) LIMITING FACTORS: REFERENCE GCCS GUIDANCE ON UN-VALIDATED PATCH INSTALLATION.

2.B.(S) OPERATIONAL IMPACTS. OPS IMPACT OF DIRECTED MEASURE IMPLEMENTATION IS MINIMAL. RESIDUAL RISK IN (***REPORTING COMPONENT***) INFORMATION NETWORKS IS DENIAL OF SERVICE ATTACK AGAINST GCCS VULNERABILITY PENDING GCCS APPROVED PATCH.

3.(S) INTELLIGENCE/RECONNAISSANCE/FORCE PROTECTION.
JTF PROVIDE LOGIC IMPLEMENTING INCREASED INFORMATION ASSURANCE MEASURES IN ADDITION TO INFOCON ALPHA DIRECTIVE MEASURES; JTF HAS DECLARED INFOCON BRAVO. REASON FOR HEIGHTENED POSTURE IS INCREASED THREAT TO ATO DISSEMINATION CAPABILITY CAUSED BY TRI-TAC INTRUSION REPORTED ABOVE.

4.(FOUO) LOGISTICS. (***REPORTING COMPONENT***) WILL INCUR ADDITIONAL COSTS FOR OVERTIME CONTRACT SYSTEM ADMINISTRATOR SUPPORT.

5. (U) COMMUNICATIONS CONNECTIVITY. NSTR.

6. (U) PERSONNEL. NSTR.

7. (U) SIGNIFICANT POLITICAL/MILITARY/DIPLOMATIC EVENTS. NSTR.

8. (S) COMMANDER'S ASSESSMENT. ESTIMATED DATE FOR FULL COMPLIANCE WITH INFOCON ALPHA IS UNKNOWN, PENDING RECEIPT AND INSTALLATION OF IAVA 2000-A-0002 PATCH FOR GCCS (REF PARA 2.A, DOD A-7). (***REPORTING COMPONENT***) ASSESSMENT OF OVERALL THREAT TO EUCOM NETWORKS IS MEDIUM. NO ADDITIONAL IMPLEMENTATION MEASURES HAVE BEEN DIRECTED FOR THE EUCOM AOR. WE CONTINUE

TO ASSESS ANY DEVELOPING LOCAL THREATS AGAINST OUR INFORMATION NETWORKS AND ARE REVIEWING LOGISTICS AND PERSONNEL REQUIREMENTS SHOULD A FURTHER INCREASE IN DOD INFOCON LEVELS BE WARRANTED.//

DECL/dd mmm yy//

(Note that the information presented in this message is notional and is for example purposes only. Paragraphs marked as classified do not contain actual classified information.)

UNCLASSIFIED

H-10. **INFOCON SITREP.** Upon collecting sufficient INFOCON-specific information from the Service/agency component Operations Centers, the HQ USEUCOM TCCC will prepare a status message, coordinated with the CND IO Cell, and transmit a INFOCON SITREP to JTF CNO using the example in Figure H-5.

Figure H-5

Example HQ USEUCOM CND SITREP

UNCLASSIFIED

(Note that the information presented in this message is notional and is for example purposes only. Paragraphs marked as classified do not contain actual classified information.)

FM HQ USEUCOM VAIHINGEN GE//ECJ6//

TO USCINCSPACE PETERSON AFB CO//CC/J6/J2/J3/SPOC WO/J39//

CJTF-CND WASHINGTON DC//J2/J3/JTFCNDWO//

INFO JOINT STAFF WASHINGTON DC//J3 NMCC//

CINCUSNAVEUR LONDON UK//00/01/019/N2/N3/N4/CDO//

CINCUSNAVEUR LONDON UK//N1/N5/N6/N7/013/018022//

HQ USAFE RAMSTEIN AB GE//CC/CV/DO/LG/SC/SCN//

USAFE AOS COMMAND POST RAMSTEIN AB GE//

HQ USAREUR HEIDELBERG GE//AEACC/AEAGC-O/AEAGD//

HQ USAREUR HEIDELBERG GE//AEAGC/AEAGB/AEAIM//

COMMARFOREUR

COMSOCEUR VAIHINGEN GE//J2/J3/J4/J6//

JAC MOLESWORTH RAF MOLESWORTH UK//CC/DO/DOI/DOO/DOT//

JAC MOLESWORTH RAF MOLESWORTH UK//SSO/ISSM/DOO/DSTS//

ODC ANKARA TU

ODC BONN GE

DISA EUR VAIHINGEN GE

HQ USEUCOM VAIHINGEN GE//ECJ6-I/ECJ6-O//

NCEUR VAIHINGEN GE//F29//

INFO AIG 996 (All ODCs)

SECRET

MSGID/SITREP/USCINCPACE//

SUBJ/SITREP/USEUCOM COMPUTER NETWORK DEFENSE (CND) SITREP(U)//

REF/A/MSG/USCINCSPACE/DOD INFORMATION OPERATIONS CONDITION (INFOCON) CHANGE TO ALPHA/999999Z XXX 00//

GENTEXT/GENERAL/
NARR/REF A IS USCINCSPACE MESSAGE DECLARING DOD INFOCON CHANGE.//
RMKS/1.(S) SITUATION/DISPOSITION/STATUS OF FORCES. USEUCOM INFORMATION NETWORKS ARE FULLY OPERATIONAL. ALL FORCES IMPLEMENTING USCINCSPACE-DIRECTED INFOCON ALPHA, EFFECTIVE 999999Z XXX 00. EXCEPTION IS 414TH SIGNAL COMPANY WHICH REMAINS AT INFOCON BRAVO DUE TO SUSPECTED INTRUSIONS INTO DEPLOYED TRI-TAC NETWORK.

2.(U) OPERATIONS.
2.A.(U) INFOCON DIRECTED MEASURE COMPLIANCE STATUS.
(U) EUCOM 1
(U) COMPLIANCE STATUS: ALL UNITS REPORT FULLY COMPLIANT

(U) ESTIMATED TIME TO COMPLETION: N/A
(U) LIMITING FACTORS: N/A

(U) EUCOM 2
(U) COMPLIANCE STATUS: ALL UNITS REPORT FULLY COMPLIANT
(U) ESTIMATED TIME TO COMPLETION: N/A
(U) LIMITING FACTORS: N/A

(U) EUCOM 3
(U) COMPLIANCE STATUS: ALL UNITS REPORT FULLY COMPLIANT
(U) ESTIMATED TIME TO COMPLETION: N/A
(U) LIMITING FACTORS: N/A

(U) EUCOM 4
(U) COMPLIANCE STATUS: ALL UNITS REPORT FULLY COMPLIANT
(U) ESTIMATED TIME TO COMPLETION: N/A
(U) LIMITING FACTORS: N/A

(U) EUCOM 5
(U) COMPLIANCE STATUS: ALL UNITS REPORT FULLY COMPLIANT
(U) ESTIMATED TIME TO COMPLETION: N/A

(FOUO) LIMITING FACTORS: CONTRACT LIMITATIONS CURRENTLY RESTRICT SYSTEM ADMINISTRATOR OVERTIME HOURS FOR SEVERAL PACOM UNITS. THESE UNITS ARE INCREASING AUDITS WHILE STAYING WITHIN CONTRACT REQUIREMENTS.

(U) EUCOM 6
(U) COMPLIANCE STATUS: ALL UNITS REPORT FULLY COMPLIANT
(U) ESTIMATED TIME TO COMPLETION: N/A
(U) LIMITING FACTORS: N/A

(U) EUCOM 7
(S) COMPLIANCE STATUS: ALL EUCOM GCCS SYSTEMS NON-COMPLIANT
(U) ESTIMATED TIME TO COMPLETION: UNK. PENDING GCCS VALIDATED PATCH TO IAVA 2000-A-0002.
(U) LIMITING FACTORS: REFERENCE GCCS GUIDANCE ON UN-VALIDATED PATCH INSTALLATION.

2.B.(S) OPERATIONAL IMPACTS. OPS IMPACT OF DIRECTED MEASURE IMPLEMENTATION IS MINIMAL. RESIDUAL RISK IN EUCOM INFORMATION NETWORKS IS DENIAL OF SERVICE ATTACK AGAINST GCCS VULNERABILITY PENDING GCCS APPROVED PATCH.

3.(S) INTELLIGENCE/RECONNAISSANCE/FORCE PROTECTION.
CJTF PROVIDE LOGIC IMPLEMENTING INCREASED INFORMATION

ASSURANCE MEASURES IN ADDITION TO DOD INFOCON ALPHA DIRECTIVE MEASURES; CJTF HAS DECLARED INFOCON BRAVO. REASON FOR HEIGHTENED POSTURE IS INCREASED THREAT TO ATO DISSEMINATION CAPABILITY CAUSED BY TRI-TAC INTRUSION REPORTED ABOVE.

4.(FOUO) LOGISTICS. USEUCOM WILL INCUR ADDITIONAL COSTS FOR OVERTIME CONTRACT SYSTEM ADMINISTRATOR SUPPORT. USCINCPAC IS ASSESSING REQUIREMENT FOR CONTINGENCY FUND SITE.

5. (U) COMMUNICATIONS CONNECTIVITY. NSTR.

6. (U) PERSONNEL. NSTR.

7. (U) SIGNIFICANT POLITICAL/MILITARY/DIPLOMATIC EVENTS. NSTR.

8. (S) COMMANDER'S ASSESSMENT. ESTIMATED DATE FOR FULL COMPLIANCE WITH DOD INFOCON ALPHA IS UNKNOWN, PENDING RECEIPT AND INSTALLATION OF IAVA 2000-A-0002 PATCH FOR GCCS (REF PARA 2.A, DOD A-7). USCINCEUR ASSESSMENT OF OVERALL THREAT TO EUCOM NETWORKS IS MEDIUM. NO ADDITIONAL IMPLEMENTATION MEASURES HAVE BEEN DIRECTED FOR THE EUCOM AOR. WE CONTINUE TO ASSESS ANY DEVELOPING LOCAL THREATS AGAINST OUR INFORMATION NETWORKS AND ARE REVIEWING LOGISTICS AND PERSONNEL REQUIREMENTS SHOULD A FURTHER INCREASE IN DOD INFOCON LEVELS BE WARRANTED. HQ USEUCOM REQUESTS NO ADDITIONAL CND-RELATED ASSISTANCE FROM USCINCSPACE AT THIS TIME.//

DECL/dd mmm yy//

(Note that the information presented in this message is notional and is for example purposes only. Paragraphs marked as classified do not contain actual classified information.)

UNCLASSIFIED

H-11**. Reporting Procedures (Local ((within USEUCOM)) INFOCON Changes).** In USEUCOM, INFOCON changes shall be implemented by operational commanders and reported through command channels (from commanders to commanders). Within HQ USEUCOM, the report of INFOCON change will be sent to the ETCC. In order to expedite processing, secure voice reports (authenticated where possible) shall be made to the unit's respective command post or operations center. The unit command post/operations center watch officer shall, in turn, immediately notify their respective Service/Agency component Operations Centers listed in paragraphs J7 a through f above. The Service/Agency component Operations Center receiving the initial report shall immediately notify all other Operations Centers listed and the HQ

USEUCOM TCCC. Notification shall be via secure telephone call followed by an immediate General text message containing the following information:

a. Organization declaring the local INFOCON change and when.

b. Brief summary of situation that led to the local INFOCON change declaration.

c. Specific actions directed as part of the local INFOCON change.

d. Additional comments from the Service/Agency-component level (e.g., is this considered an isolated incident?)

H-12. **HQ USEUCOM J39 IOWG Reports.** After receiving notification from the Service/Agency component Operations Center, the HQ USEUCOM CND IO Cell will send a voice report to USCINCSPACE. As soon as possible thereafter the CND IO Cell will coordinate with the IOWG to obtain ECJ3 approval of the general text message (Fig H-6).

Figure H-6
Example INFOCON Change Communications Report

UNCLASSIFIED

(Note that the information presented in this message is notional and is for example purposes only. Paragraphs marked as classified do not contain actual classified information.)

FM HQ USEUCOM VAIHINGEN GE//ECJ3//

TO USCINCSPACE PETERSON AFB CO//CC/ J6/J2/J3/SPOC WO/J39//

CJTF-CND WASHINGTON DC//J2/J3/JTF-CND WO//

INFO JOINT STAFF WASHINGTON DC// NMCC//

CINCUSNAVEUR LONDON UK//00/01/019/N2/N3/N4/CDO//

CINCUSNAVEUR LONDON UK//N1/N5/N6/N7/013/018022//

HQ USAFE RAMSTEIN AB GE//CC/CV/DO/LG/SC/SCN//

USAFE AOS COMMAND POST RAMSTEIN AB GE//

HQ USAREUR HEIDELBERG GE//AEACC/AEAGC-O/AEAGD//

HQ USAREUR HEIDELBERG GE//AEAGC/AEAGB/AEAIM//

COMMARFOREUR

COMSOCEUR VAIHINGEN GE//J2/J3/J4/J6//

JAC MOLESWORTH RAF MOLESWORTH UK//CC/DO/DOI/DOO/DOT//

JAC MOLESWORTH RAF MOLESWORTH UK//SSO/ISSM/DOO/DSTS//

ODC ANKARA TU

ODC BONN GE

DISA EUR VAIHINGEN GE

HQ USEUCOM VAIHINGEN GE//ECJ6-I/ECJ6-O//

NCEUR VAIHINGEN GE//F29//

INFO AIG 996 (All ODCs)

CINCS

SERVICES

AGENCIES

SECRET
MSGID/OPREP-3TB/HQ USEUCOM/J39 IO CELL/001/AUG00//
SUBJ/USASOC INFOCON CHANGE NOTIFICATION (U)//
REF/A/MSG/USAFE CSS INFOCON CHANGE (U)/052329Z AUG 00//
GENTEXT/GENERAL/

1. (U) ORGANIZATION DECLARING INCIDENT:

2. (U) DATE, TIME AND DURATION OF INCIDENT: USAFE CSS INFOCON CHANGE NOTIFICATION MESSAGE, 052329Z SEP 00.

A. (U) NEW INFOCON: BRAVO

B. (U) OLD INFOCON: ALPHA

3. (S) INCIDENT DESCRIPTION. PROTECTED DISTRIBUTION SYSTEM (PDS) ASSOCIATED WITH TACTICAL PACKET NETWORK (TPN) MOBILE SUBSCRIBER EQUIPMENT (MSE), CURRENTLY DEPLOYED TO BOSNIA, ASSESSED AS COMPROMISED. INITIAL ASSESSMENT INDICATES INTRUDER

MAY BE ASSOCIATED WITH HACKER GROUP SUPPORTING COUNTRY ORANGE. CLASSIFICATION OF NETWORK IS SECRET/RELEASABLE TO COALITION FORCES.

4. (S) DAMAGE ASSESSMENT AND OPERATIONAL MISSION IMPACT. OPERATIONAL IMPACT OF ACTIVITY IS SERIOUS; LOSS ASSESSMENT ONGOING. COUNTRY ORANGE MAY HAVE ACCESSED OPERATIONS AND INTELLIGENCE INFORMATION RELATED TO COALITION FORCES MISSION EXECUTION.

5. (U) ACTIONS.

A. (FOUO) ACTIONS TAKEN. DIRECTED IMPLEMENTATION OF ALL DOD INFOCON BRAVO ACTIONS WITH PRIORITY ON COMSEC MONITORING AND EVALUATION OF TABI/TSABI DEVICES. ADDITIONALLY, A TECHNICAL SURVEILLANCE COUNTERMEASURES (TSCM) SURVEY OF THE NETWORK HAS BEEN DIRECTED.

B. (FOUO) EXIT CRITERIA. HQ USAFE SHALL ASSESS THE REQUIREMENT TO REMAIN AT INFOCON BRAVO WEEKLY (AT A MINIMUM). CRITERIA FOR DETERMINING WHETHER TO EXIT BRAVO SHALL INCLUDE A CHANGE (INCREASE OR DECREASE) OF ADVERSARY CAPABILITY AND INTENT, AND/OR CLOSURE OF EXPLOITABLE VULNERABILITIES.

6. (S) COMMANDER'S ESTIMATE. ALL OPERATIONAL SYSTEMS REMAIN FULLY CAPABLE. PERSONNEL ARE STILL CONDUCTING AN ASSESSMENT TO DETERMINE THE EXTENT OF POTENTIAL INFORMATION COMPROMISE. HQ USAF HAS CONSIDERED THE REQUIREMENT TO DIRECT AN AF WIDE INFOCON CHANGE TO BRAVO, BUT HAS DETERMINED THIS MEASURE IS NOT WARRANTED AT THIS TIME. HQ USEUCOM CONTINUES TO EVALUATE THE SITUATION AND WILL DIRECT A CORRESPONDING INFOCON CHANGE WHEN/IF NECESSARY.

7. (U) ADDITIONAL COMMENTS. N/A.

8. (U) POC INFORMATION.

DECL/dd mmm yy//

(Note that the information presented in this message is notional and is for example purposes only. Paragraphs marked as classified do not contain actual classified information.)

UNCLASSIFIED

H-13. **Sharing INFOCON Changes with NATO and Coalition Partners.** The INFOCON process governs only systems that are owned and operated by the U.S. DoD. However, because some DoD networks interface with allied/coalition networks, the INFOCON system does have the potential to impact these external networks. The interface with these systems, and correspondingly, the potential impact of INFOCON, occurs via the implementation of secure gateways and SABI/TSABI connections. The directive actions at each INFOCON level require commanders to conduct a risk assessment and perform heightened security on SABI/TSABI interfaces, including those interfaces with allied/coalition networks. Commanders who determine the disposition and/or configuration of SABI/TSABI devices must coordinate INFOCON measures with commanders and system administration personnel of the interfacing networks. Commanders are encouraged to share INFOCON declarations and directive measures with allied/coalition partners (as permitted by intelligence/security restrictions). Commanders of these networks should be encouraged to apply similar measures, as applicable.

H-14. **Security.** Classification guidance and disclosure policy concerning IO is addressed in DoDI 3600.2. Specific guidance related to INFOCON follows.

a. INFOCON levels combined with descriptions are For Official Use Only (FOUO).

b. General criteria to declare an INFOCON are Confidential. Specific criteria may be published in a classified appendix, if required.

c. Defensive measures, when not tied to a specific INFOCON, are unclassified.

d. Individual INFOCON measures to be taken by all personnel, regardless of INFOCON, are unclassified.

e. A combatant command, Service, or agency may authorize release of its INFOCON system and procedures to allies or coalition partners as necessary to ensure effective protection of its information systems. Locally developed INFOCON procedures should use DoDI 3600.2 and the above guidance when considering release to allies or coalition partners.

f. Changes in INFOCON are Operations Security (OPSEC) indicators and/or Essential Elements of Friendly Information (EEFIs), and must be protected accordingly. The criteria and response measures are also of value to foreign intelligence services in assessing the effectiveness of a CNA or CNE and in analyzing DoD's response. Do not post INFOCON procedures in publicly accessible locations.

H-15. **DOD Directive Actions.** In order to comply with DOD classification guidance, DOD Directive Actions supporting the five levels of INFOCONS will not be published in distributed hard copies of this directive. However, the electronic version of ED 25-5 posted on the SIPRNET at http://www.eucom.smil.mil/ecj6-i/pubs/eucom_pubs/eucom_pubs.htm is linked to the draft directive actions. (NOTE: This function will be available once the new ED 25-5 is published. We are still awaiting the final DOD Directive Actions to be published by Joint Staff).

Appendix H - Information Conditions (INFOCONS)

Annex A – EUCOM INFOCON Response Measures

(U) INFOCON RESPONSE MEASURES

Establishing an INFOCON does not presuppose a certain set of response measures are activated. Upon declaration of an INFOCON level, HQ USEUCOM will direct specific defensive measures (listed below) for implementation within the theater based on the threat and the situation. Any of the listed response measures may be directed at any INFOCON level. Component, Subordinate UNIFIED, JTF, and local Commandeers will not direct a less restrictive INFOCON response measure than that set by HQ USEUCOM. Upon publication of CJCSM 6510.01, HQ EUCOM will review and revalidate the INFOCON processes and measures for consistency.

1. (FOUO) Verify USEUCOM IO point of contact list of phone numbers, e-mail addresses, and official message traffic address list. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

2. (FOUO) Alert Intelligence Community to monitor threat for additional DIO indications and warnings (I&W), and increased foreign intelligence and information activity. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

3. (FOUO) Issue status report of activities to the USEUCOM TCCC as directed in the INFOCON change message in accordance with report format in Figure H-4. (Component, Subordinate Unified, and JTF Commands)

4. (FOUO) Ensure all Commanders, Security Managers, Information system Security Managers (ISSM), Information system Security Officers (ISSO), System Administrators (SA), COMSEC Custodians, and other communications or information systems organizations or personnel are briefed on the threat activity, INFOCONS changes, and response measures. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands.)

5. (FOUO) Increase OPSEC awareness. Include things such as reminding all users of the risks of being monitored by adversaries during e-mail and phone use (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

6. (FOUO) Remind all users to immediately report any suspicious or unauthorized requests for direct access or computer passwords to access C4I networks and workstations. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

7. (FOUO) Remind all users to report unusual network/computer activity, viruses, and potential denial of services (DoS) attacks of computer, radiotelephone, satellite, or telephone systems (including FAX machines). Report unusual activity in accordance with established

USEUCOM and local incident reporting procedures. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

8. (FOUO) Verify all dial-in/dial-out capabilities are removed from LAN workstations. Only stand-alone workstations will be used for Fax and answering machine capabilities. (HQ USEUCOM, Component, Subordinate Unified and JTF Commands)

9. (FOUO) Update and distribute list of intruder Internet Protocol (IP) addresses for local IP hotlists. If current threat source is known, ensure routers and/or firewalls block appropriate Internet Protocol (IP) hotlist address listings. Monitor and log activity as appropriate. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

10. (FOUO) Update attack signatures, profiles, and methods of recent attacks for use by intrusion detection systems, and for use by IA professionals to manually detect intrusions. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

11. (FOUO) Update all virus software and signature files. (HQ USEUCOM, Component, Subordinate Unified and JTF Commands)

12. (FOUO) Validate the operation of server system log files, and in addition to daily reviews, review firewall and intrusion detection logs for evidence of specified unusual or malicious activity. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

13. (FOUO) Ensure routers and firewalls protecting C4I networks have proper configuration settings to guard against known vulnerabilities and methods of recent attacks. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

14. (FOUO) Direct all users to conduct a key update of their secure voice devices (STU, STE, Iridium, Sectera, etc.). (HQ USEUCOM, Component, Subordinate Unified and JTF Commands)

15. (FOUO) Require all computer systems users to change passwords. Passwords will be changed every 90 days while in INFOCON Alpha; every 30 days while in INFOCON BRAVO, CHARLIE, or DELTA. (HQ USEUCOM, Component, Subordinate Unified and JTF Commands)

16. (FOUO) Verify current list of all SABI/TSABI interconnections, and status of accreditation packages for same to HQ USEUCOM TCCC (tccc@eucom.smil.mil (SIPR); tccc@eucom.mil (NIPR)). (HQ USEUCOM, Component, Subordinate Unified and JTF Commands)

17. (FOUO) Run password evaluation tools against system password databases to ensure compliance with minimum DoD standards. (HQ USEUCOM, Component, Subordinate Unified and JTF Commands)

18. (FOUO) Conduct vulnerability assessment to verify and report application of all known and approved operating system patches, fixes, and new releases, to include applicable IAVAs and IAVBs, to the USEUCOM ISSO/ISSM. (HQ USEUCOM, Component, Subordinate Unified and JTF Commands)

19. (FOUO) Conduct a targeted vulnerability scan/assessment to identify/verify that a specific patch/hot fix has been applied. Specific patch would be threat related. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

20. (FOUO) Report status of any systems that are non-compliant with IAVA alerts. Include those systems that have applied for waivers from the DAA. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

21. (FOUO) Close all remote maintenance ports on vulnerable or affected routers, firewalls, servers, computer-based telephone switches, and any other accessible information systems. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

22. (FOUO) Verify real-time audit analysis capabilities, if available, are turned on and monitored. Alarm levels of Automated Intrusion Detection Systems should be adjusted to provide appropriate alert thresholds. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

23. (FOUO) Impose minimize conditions on messaging, e-mail, and worldwide web access (NIPRNet and SIPRNet). (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

24. (FOUO) Validate a plan for JCMA COMSEC monitoring support for HQ USEUCOM and components. (ECJ6)

25. (FOUO) Examine operational impacts of, disconnecting all SABI/TSABI bridges between classified and unclassified networks, and/or between classified and allied networks. (HQ USEUCOM IOC & ECJ6; Components, Subordinate Unified and JTF Commands)

26. (FOUO) Reduce dial-in access, to include RASP, on both the NIPRNet and SIPRNet to minimum essential personnel. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

27. (FOUO) Reduce remote user access to web-based e-mail to minimum essential personnel. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands).

28. (FOUO) For the conduct of official business, maximize the use of approved secure modes of information exchange, such as secure telephones (STU/STE), secure FAX, and SIPRNET-based systems such as Global Command and Control System (GCCS). (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

29. (FOUO) Evaluate the operational impact of restricting information exchange to ONLY secure modes.(i.e. STU/STE, secure fax, SIPRNet ONLY)

30. (FOUO) Review/validate the plan for disconnection of non-mission essential systems. (HQ USEUCOM, Component, Subordinate Unified and JTF Commands)

31. (FOUO) In the case of a confirmed computer network attack, users of the affected workstations, and the respective ISSM and ISSO, will isolate the affected workstation or network, and ensure evidence is maintained to pass to law enforcement agencies/counter intelligence. Notify chain of command. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

32. (FOUO) Disconnect Secure Mail Guards (SMG) or any other SABI/TSABI device between unclassified and classified LANs, or networks of different classifications. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

33. (FOUO) Power down all network devices not in use. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

34. (FOUO) Disconnect any non-mission essential SABI/TSABI connections between classified and allied networks. (HQ USEUCOM, Component, Subordinate Unified and JTF Commands)

35. (FOUO) Review options, and impacts of, disconnecting all critical C4I systems, networks and workstations capable of operating in a stand-alone mode, from the NIPRNet. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

36. (FOUO) Review options, and impacts of, disconnecting all critical C4I systems, networks and workstations capable of operating in a stand-alone mode, from the SIPRNet. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

37. (FOUO) Disconnect all non-mission essential subnetworks from the HQ USEUCOM unclassified LANs. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

38. (FOUO) Disconnect all non-mission essential subnetworks from the HQ USEUCOM classified LANs. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

39. (FOUO) Conduct vulnerability assessment of any remaining operational interconnections. (HQ USEUCOM, Component, Subordinate Unified and JTF Commands)

40. (FOUO) Conduct review of all COMSEC key management plans, and prepare implementation of full re-key of minimum critical networks and systems. (ECJ6)

41. (FOUO) Implement manned 24x7 monitoring of all network servers, guards, filters, firewalls and other activity logs for suspicious or unusual activity. (HQ USEUCOM, Component, Subordinate Unified and JTF Commands)

42. (FOUO) Implement plan for disconnection of all non-mission essential systems. (HQ USEUCOM, Component, Subordinate Unified and JTF Commands)

43. (FOUO) Deny ALL access to the public unclassified Web servers. (HQ USEUCOM, Component, Subordinate Unified and JTF Commands)

44. (FOUO) Configure perimeter security devices to allow access to only official addressees (i.e. gov, mil, etc) on the NIPRNet. (HQ USEUCOM, Component, Subordinate Unified and JTF Commands)

45. (FOUO) Restrict all email use to mission essential personnel only. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

46. (FOUO) Remove ALL dial-in access to unclassified LANs. (HQ USEUCOM, Component, Subordinate Unified and JTF Commands)

47. (FOUO) Remove ALL dial-in access to classified LANs, including RASP. (HQ USEUCOM, Component, Subordinate Unified and JTF Commands)

48. (FOUO) Disconnect ALL NIPRNET access at the DISN router. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

49. (FOUO) Disconnect ALL SIPRNET access at the DISN router. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

50. (FOUO) Disconnect all critical C4I systems, networks and workstations capable of operating in a stand-alone mode. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

Appendix I

Communications Security Releases to Foreign Nations

I-1. **CINC COMSEC Release Request (CRR).** All units operating in the USEUCOM AOR under conditions requiring a release of US COMSEC products or associated COMSEC information to a NATO or non-NATO country shall forward pertinent information to HQ USEUCOM through their respective Service component headquarters. Information shall be submitted as a free text electrical message to HQ USEUCOM ECJ5 with an information copy to ECJ6-I (Internal HQ USEUCOM staff directorates may use an SSRS). The following minimum information is required to support HQ USEUCOM initiation of a CINC CRR:

a. Type of CRR: Request in Principle (RIP) or Request in Specific (RIS). If a RIS, identify the quantity of COMSEC products (to include spares) needed to support the secure interoperability requirement.

b. Define the interoperability requirement to be supported (If request is related to a CONPLAN, OPLAN, etc., identify).

c. Specify the scope, duration, and urgency of the requirement.

d. Identify whether the foreign government has previously signed a Communications Interoperability and Security Memorandum of Agreement (CIS MOA) and whether a US Government Foreign Military Sales (USG FMS) DoD COMSEC account is required; if so, whether it is currently operational.

e. If a signed CIS MOA does not exist, specify timeline for HQ USEUCOM to draft, get delegated approval to negotiate, negotiate, and conclude a CIS MOA.

f. Discuss the provisions for providing engineering, installation, maintenance, key, and logistic support for the released COMSEC products or associated COMSEC information.

g. Identify any requirements for instructional material translation such as one-for-one replacement instructions, operator, and limited maintenance manuals to be provided to the foreign country. (Note: Maintenance of released COMSEC equipment is restricted to US government personnel only.)

h. Discuss the concept for crypto net management.

i. Remarks: amplifying free text.

I-2. **CINC CRR Coordination Process.**

a. The appropriate ECJ5 Country Team shall evaluate the information provided to determine if there is an emerging or currently documented interoperability requirement with the country in question.

b. If the secure interoperability requirement is determined valid, ECJ5 shall draft and staff the CINC CRR IAW Ref. A-15.

c. If the CINC CRR involves an actual equipment release and has been approved by the NSTISSC, the originating entity must coordinate with DIRNSA I11 to effect the provisioning, installation, training, and operation of the equipment and associated cryptographic material. HQ USEUCOM ECJ5 and ECJ6-I shall be kept informed throughout this process.

I-3. **Ship-Rider Procedures.** "Ship-rider" procedures are a DIRNSA-approved COMSEC waiver used to solve interoperability requirements for ongoing combined operations or combined training exercises. The procedure requires US cleared personnel to temporarily install, operate, key and physically secure US COMSEC equipment in a non-NATO foreign government weapon or C4I system located in a foreign site or mobile platform. The USEUCOM component commands shall submit ship-rider requests IAW appendix B to enclosure B to ref A-15. HQ USEUCOM ECJ6-I shall be an information addressee on all requests.

I-4. **Approval for Urgent Requirements.** In the USEUCOM AOR, secure interoperability requirements with non-NATO foreign governments shall be satisfied using ship-rider procedures wherever possible. In situations where US lives may be at risk and circumstances disallow CINC CRR processing or ship-rider procedures, units are authorized to submit urgent COMSEC release requests directly to DIRNSA I11, info the component command headquarters and HQ USEUCOM, ECJ6-I.

I-5. **Discussions with Foreign Nations.** Before initiating discussions or negotiations on weapon systems, C4I systems, or other platforms, all USEUCOM units must define the requirement, or emerging requirement, for US COMSEC equipment. When use of US COMSEC products or associated COMSEC information is implied or possible (i.e., major weapons systems like the F/A-18), but not absolutely required, discussions may be conducted. However, no COMSEC products or associated COMSEC information may be committed or discussed other than to acknowledge that some type US or authorized/approved commercial COMSEC equipment may be required. An approved RIP (see Ref. A-15) is required before initiating discussions on disclosure or release of specific US COMSEC information to a non-NATO foreign government.

Appendix J

Joint Key Management

J-1. **General.** This appendix prescribes policy and procedures for the management of contingency COMSEC keying materials (hereafter referred to as "key") employed to support joint operations and exercises. Currently, there are three sources of contingency key available in the USEUCOM AOR:

a. The Joint Inter-theater COMSEC Package (JICP)

b. Key generated IAW rules and procedures prescribed in NAG-16

c. The Electronic Key Management System (EKMS)

J-2. **Policy.** Key used to support joint contingencies and exercises shall be generated as closely as possible to the time of need and distributed in response to validated network requirements. Provisions for electronic key generation/distribution shall be made during the planning stages of operations and exercises.

J-3. **Joint Inter-theater COMSEC Package (JICP).**

a. In the USEUCOM AOR, the JICP shall be used as a source of backup key. Wherever possible, JICP key shall be held in contingency-cache accounts from which they can be electronically distributed to authenticated users as required.

b. JICP validations shall be approved based upon joint requirements. During the validation process, care shall be taken to match JICP short titles to their respective cryptographic hardware and classification requirements. (i.e., USKAT-1019 is a KY-57/58 key used to encrypt SECRET-level and below information. USKAT-1019 shall not be assigned for use with any other cryptographic device or to encrypt information classified higher than SECRET)

c. All new JICP key validations shall be coordinated with HQ USEUCOM, ECJ6-I through the respective component command headquarters.

d. Components and supporting elements shall promulgate unit-level guidance for employing JICP call-out messages. (Note: Announcing the intended use of any symmetric key is a practice dangerous to security. If used, call-out messages shall be transmitted via secure means only and only after other means of coordination have been exhausted.)

J-4. **Field Generation and Over-the-Air Distribution (OTAD) of COMSEC Key in Support of Tactical Operations and Exercises.**

a. In USEUCOM, NAG-16 OTAD (Ref. A-42) shall be used wherever EKMS services are unavailable and wherever OTAD can be used to avoid pre-positioning physical key. Components and supporting elements shall ensure that all deployable communications O&M activities are trained in NAG-16 procedures and written instructions are in place to support any unique OTAD requirements. All units operating in the USEUCOM AOR shall ensure they have access to the following items prior to deployment:

(1). OTAD-Capable DTD

(2). STU-III/STE Connector Cable

(3). Fill Cable

b. The US Army Theater COMSEC Management Office - Europe (USATCMO-E) located at Coleman Barracks in Mannheim Germany supports HQ USEUCOM by providing limited contingency OTAD support for joint deployments and exercises. Units requiring contingency OTAD services should send a free-text electrical message to USATCMOEUR 11THSIGDET MANNHEIM GE info HQ USEUCOM VAIHINGEN GE//ECJ6-I//. Messages requesting joint exercise support shall be sent a minimum of ten days prior to STARTEX.

J-5. **Joint EKMS.** Components and supporting elements shall insure Local Operating Instructions (LOIs) covering joint EKMS support requirements are available at EKMS Tier-2 accounts supporting deployable units and missions. As a minimum, LOIs shall address the following:

(1). Procedures for promulgating/responding to COMSEC Alert Messages

(2). Procedures to be taken when directed to assume the role of CINC or CJTF workstation.

(3). Procedures and guidance for local key generation (ALC-7) and distribution procedures required to support USEUCOM policy stated in paragraph J-2 above.

(4). Guidance for protecting and controlling deployed electronic key storage devices.

J-6. **EKMS Extension Tier-1 Segment (ETIS).** As the primary focal point for joint EKMS support in the USEUCOM AOR, the ET1S shall:

a. Serve as the center for all supporting-CINC key requirements to include posting of ALC-7 key with the CONUS Tier-1.

b. Develop contingency plans for sustaining joint EKMS support in the absence of CONUS Tier-1 connectivity.

c. Serve as the primary contingency-cache account for JICP key and NATO/allied materials required by U.S. Forces.

Annex A to Appendix J

COMSEC Alert Messages

COMSEC Alert Messages shall be used to define a contingency Key Distribution Plan (KDP) and assign responsibilities to all KDP-support elements. Messages shall be classified according to content and electronically disseminated via secure means only. Message shall be sequentially numbered and updated as the contingency or exercise develops and new information is obtained.

Sample COMSEC Alert Message

```
FM: USAFE CSS RAMSTEIN AB GE//SCBI//
TO: USATCMO-E 11TH SIG DET MANNHEIM GE//ET1S//
CDR 587THSIGCO VAIHINGEN GE//EKMS ACCOUNT #//
1CCSQ RAMSTEIN AB GE//EKMS ACCOUNT #//
OIC CMDSA SHAPE BE//REGIONAL //EKMS ACCOUNT #//
COMSOCEUR VAIHINGEN GE//REGIONAL //EKMS ACCOUNT #//
CDR OPMAS-E DCS STA LANDSTUHL GE//EKMS ACCOUNT#//
ASC RAF CROUGHTON UK//EKMS ACCOUNT #//
ASC PIRMASENS GE//EKMS ACCOUNT #//
CINCUSAREUR HEIDELBERG GE//EKMS ACCOUNT #//
CINCNAVEUR LONDON UK//EKMS ACCOUNT #//
HQ USAFE RAMSTEIN AB GE//EKMS ACCOUNT #//
HQ MARFOREUR BOEBLINGEN GE//EKMS ACCOUNT #//
DISAEUR VAIHINGEN GE//EKMS ACCOUNT #//
CDR5THSIGCMD MANNHEIM GE//EKMS ACCOUNT #//
(ALL UNITS IDENTIFIED IN THE OPLAN/OPORD/DEPLOYMENT ORDER AND THEIR
EKMS ACCOUNT NUMBERS IF KNOWN)
INFO:
HQ USEUCOM VAIHINGEN GE//ECJ6-I/ECJ36//
SUPPORTING CINCS
MAJOR COMMANDS
JOINT COMSEC MANAGEMENT OFFICE MACDILL AFB FL
DIR CRYPTO MGT KELLY AFB TX //PT1S-K//
DIRUSACCSLA FT HUACHUCA AZ //PT1S-H//
DCMS WASHINGTON DC (OR TIER 1/ET1S)
JOINT STAFF WASHINGTON DC
DIRNSA FT GEO G MEADE MD
CDRJCSE MACDILL AFB FL
(AS REQUIRED)
BT
(CLASSIFICATION ACCORDING TO CONTENT)
SUBJECT: (CONTINGENCY/EXERCISE NAME, COMSEC ALERT#/MONTH/YEAR -
EXAMPLE:  PROVIDE COMFORT COMSEC ALERT 01/03/01)
```

REF A. OPLAN/EXERCISE ORDER

REF B. DEPLOYMENT ORDER

REF C. ED25-5

1. () PURPOSE OF THIS MESSAGE IS TO PROMULGATE THE INITIAL PROVIDE COMFORT KEY DISTRIBUTION PLAN (KDP). REQUEST WIDEST POSSIBLE DISSEMINATION OF THIS MESSAGE AND ANY FOLLOW ON COMSEC ALERTS RELEASED IN ORDER TO UPDATE KDP INFORMATION PROVIDED HEREIN.

2. () THE ETIS 1S IS HEREBY ALERTED TO PROVIDE KDP SUPPORT FOR PROVIDE COMFORT AS DEFINED IN REF C. CONTACT INFORMATION FOR ET1S OPERATIONS FOLLOWS:

A. () KDP ASSISTANCE: (CONTACT INFO)

B. () EKMS/NAG-16 OTAD: (CONTACT INFO)

C. () NATO/ALLIED KEY: (CONTACT INFO)

D. () NON-TRADITIONAL KEY: (CONTACT INFO)

E. () GENERAL HELP DESK: (CONTACT INFO)

3. () THE BELOW LISTED EKMS ACCOUNTS HAVE BEEN DESIGNATED CINC/CJTF WORKSTATIONS. CUSTODIANS SHALL ENSURE EKMS CREDENTIALS ARE POSTED AS REQUIRED FOR INTEROPERABILITY WITH THE ET1S, SUPPORTING EKMS ACCOUNTS IDENTIFIED IN PARAGRAPHS 4 THROUGH ___ BELOW, AND OTHER DEPLOYED SERVICE TIER-2 ACCOUNTS AS REQUIRED BY THE MISSION:

A. () CINC WORKSTATION (IF MORE THAN ONE IS ASSIGNED, LIST IN SUBPARAGRAPHS):

(1) () EKMS ACCOUNT #
(2) () CUSTODIAN NAME
(3) () CONTACT INFORMATION

B. () CJTF WORKSTATION (IF MORE THAN ONE IS ASSIGNED, LIST IN SUBPARAGRAPHS):

(1) () EKMS ACCOUNT#
(2) () CUSTODIAN NAME
(3) () CONTACT INFORMATION

4. () ALC-7 KEY IS REQUIRED TO SUPPORT NETWORK/SYSTEM-A AS FOLLOWS:

A. () CCI (KG-84, KY-57, ETC.)

B. () CLASSIFICATION

.C. () NUMBER OF SEGMENTS

D. () SEGMENT EFFECTIVE PERIODS

(1). () SEGMENT ONE: (EFFECTIVE DATES)

(2). () SEGMENT TWO: (EFFECTIVE DATES)

E. () DISTRIBUTION PROFILE FOR NETWORK/SYSTEM-A:

(1) () SUPPORTING EKMS ACCOUNT FOR USER/MEMBER-A OF NETWORK/SYSTEM- A

(2) () SUPPORTING EKMS ACCOUNT FOR USER/MEMBER-B OF NETWORK/ SYSTEM-A

(3) () CONTINUE UNTIL ALL USER/MEMBERS OF NETWORK/SYSTEM-A HAVE BEEN IDENTIFIED IN THE DISTRIBUTION PROFILE.

5. () ALC-7 KEY IS REQUIRED TO SUPPORT NETWORK/SYSTEM-B AS FOLLOWS: (REPEAT ABOVE PATTERN OF KEY IDENTIFICATION AND DISTRIBUTION FOR NETWORK/SYSTEM-B, C, ETC.)

6. () ALL SUPPORTING CINC FORCES ARE REQUIRED TO DEPLOY WITH (OR HAVE ACCESS TO) THE FOLLOWING MINIMUM ITEMS:

A. () DATA TRANSFER DEVICE

B. () FILL CABLE

C. () STU/STE CONNECTOR CABLE

7. () PKI REQUIREMENTS: IDENTIFY ANY KNOWN REQUIREMENTS FOR DEPLOYED CA/RA/IECA/TA FUNCTIONS.

8. () IAVA/INFOCON REPORTING REQUIREMENTS

9. () AMPLIFYING DATA DEEMED NECESSARY BY THE PROMULGATING UNIT (I.E., HJ TIMES, COMPROMISE RECOVERY PROCEDURES, PROCEDURES FOR TRANSFERRING TO CONTRACTOR SUPPORT, SPECIAL KEY ORDERS FROM

CENTRAL FACILITY, ALLIED KEY HANDLING INSTRUCTIONS, ETC).

Annex B to Appendix J

COMSEC Appendices

Joint key management shall be addressed in all OPLANs, either as an internal portion of the C3S annex or as an appendix. The COMSEC appendix must clearly describe the mission, the supporting units, and the role each unit will play in the key management process. The sample COMSEC Appendix provided below was written in the format recommended in the Joint Operation Planning and Execution System (JOPES) Volume II (Ref A-18).

Sample COMSEC Appendix

( ) REFERENCES:

(a) DOD D-5200.5, Communications Security (COMSEC)
(b) CJCS INST 6510.01, Joint and Combined Communications Security
(c) MCM-SYP-106-93, Implementation of Over the Air Key Distribution
(d) NAG-16/TSEC, Field Generation and Over the-Air Distribution of COMSEC Key in Support of Tactical Operations and Exercises (List other documents that support the operation/exercise)
(e) USACOMINST C2281.1
(f) DoD X.509 Certificate Policy
(g) European Directive (ED) 25-5

1. () Purpose: Summarize the operational situation in relation to available threat information.

2. () General: Briefly state the requirement to employ confidentiality, authentication, and non-repudiation controls to protect networks and information systems.

3. () Operations: Define the roles and responsibilities of the following:

a. () CINC Workstation(s): Identify EKMS account(s) tasked to support HQ USEUCOM ECJ3 requirements.

b. () CJTF Workstation(s): Identify EKMS account(s) tasked to support the contingency or exercise Key Distribution Plan (KDP).

c. () Key Management Infrastructure (KMI) Support: Normally, KMI support should be available through organic unit assets (personnel & equipment). Should additional support be required for large operations, identify personnel & equipment (by Service, grade, occupational specialty, etc.). Consider manning for CJTF workstations, Certificate Authority (CA) workstations, Registration Authority (RA) functions, Interim External Certificate Authority (IECA) functions, and Trusted Agent (TA) functions.

d. () ET1S: Identify the ET1S' role in providing contingency KDP support. Specifically, address posting of contingency key with the CONUS Tier-1 for "supporting-CINC" forces.

e. () JICP: Identify cache accounts available for contingency over-the-air distribution (OTAD) of JICP or other physical key.

4. () Responsibilities: Define the roles of the supporting and the supported Major Operational COMSEC Authorities. For most NATO operations (unless requested by NATO to take the COMSEC lead) the U.S. will be in a supporting role.

5. () Execution: Outline any special support that may be required to sustain joint key management operations. For example:

a. () KMI support team configurations, reporting instructions, reporting dates, etc.

b. () Requirements for Joint COMSEC Monitoring Activity (JCMA) support.

c. () Information Assurance Vulnerability Assessments (IAVAs) and INFOCON reporting requirements.

d. () Secure-voice requirements.

e. () OTAD instructions. (Reiterate the need for supporting forces to deploy with DTDs, fill cables, and STU/STE connector cables.)

6. () Coordinating Instructions: Provide for specific coordination among activities concerned.

a. () Specify any reporting/coordination required of deployed elements supporting Service-unique systems or networks.

b. () Identify the process for coordinating release of NATO/allied COMSEC for U.S. Forces.

c. () Identify secure links (STU-III, STE, TACSAT, INMARSAT, etc.) for EKMS and NAG-16 OTAD support.

7. () Administration and Logistics.

a. () Specify any requirements for operational logs (e.g. NAG-16) to track generation, distribution, and destruction of key.

b. () Identify operations codes, auto-manual systems, call-sign documents and authenticators (Required for use on unsecured networks only).

8. () Command and Control.

a. () Provide instructions for recovering from and reporting possible key compromises.

b. () Provide key-disposition instructions for redeployment or for transition to commercial/contract-communications support.

Appendix K

The DoD Public Key Infrastructure

K-1. **General.** Requirements for a Public Key Infrastructure (PKI) derive from the need to defend electronic communications and computing systems from acts such as blocking, interception, tampering, destruction, and forgery. In response to such threats, the DoD is developing a PKI consisting of products and services designed to manage X.509 certificates and related cryptographic key. This appendix supplements guidance provided in the DoD X.509 Certificate Policy document.

K-2. **Policy.**

a. Portions of the PKI shall be configured and available to support the needs of deployed USEUCOM forces. Those deployable elements shall be transported using organic assets or normal transport means of the units with which they are associated.

b. Deployable PKI components shall operate using the same power used by the associated deployed forces for their organic communications and information systems equipment.

c. PKI supporting closed tactical networks shall provide interoperability with allied systems used in the deployed operational environment.

d. Components and supporting elements shall develop plans for subordinate units utilizing PKI support in closed tactical networks. Plans shall address the need for rapidly replacing lost or destroyed user tokens.

e. PKI support to closed networks shall not depend on any form of reach-back communications or other connectivity to fixed networks such as NIPRNET or SIPRNET.

f. Where an isolated Coalition Wide Area Network (WAN) is established, the Registration Manager (RM), the directory, and the Certificate Authority (CA) shall be on the isolated network and directory services must be a part of the isolated network environment. Use of deployable CA and RM workstations will also help to minimize bandwidth loading.

g. Allied and contractor certificates shall be generated to cover the duration of an operation or exercise. Additional security precautions such as ACLs should be employed where necessary to protect sensitive operational information.

h. Component public key implementers shall work closely with system administrators and the IA community to ensure private keys and pass phrases cannot be recovered through the use of remote administrative tools.

i. To protect against duping and "forged signature" attacks, two-way authentication shall be required between certificates employing device addresses.

j. Access to key management services (e.g., human-readable cryptographic products, key, certificates, key-recovery services, etc.) shall be based upon human-user privileges. Access to unencrypted operational key shall require a Class 5 token.

k. In addition to key and key-product services, all USEUCOM regional KMI enclaves shall provide the following as a minimum:

(1). Certificate registration and verification services.

(2). KMI Library services (On-line access to operational procedures, reference manuals, policy documents, etc.)

(3). Cross certification and connectivity services.

(4). Risk assessment and mitigation guidance.

(5). Key tracing services.

(6). Compromise recovery support.

l. Distribution of private keys generated by PKI shall be protected with authentication, integrity, and confidentiality controls.

m. Component PKI implementers shall ensure the following:

(1). Processes for key recovery are well documented and readily available to PKI operators, users, and relying parties.

(2). Deployable PKIs have no single points-of-failure that could make CA services unavailable.

(3). PKIs are designed to operate in the face of denial-of-service attacks.

(4). PKIs are fully integrated with available DoD standard systems for network monitoring and defense.

(5). PKI - core components are protected by a standard suite of network security components (e.g., firewall technology, malicious code detectors, network and host-based Intrusion Detection Systems).

(6). Float systems are available for immediate backup.

(7). Contractor personnel are fully trained in the technology, policies, and operating procedures of PKI, and are fully cognizant of their responsibilities under the DoD CP.

(8). Critical PKI components such as CAs are housed in facilities with strong physical security protections.

n. PKIs shall not require the use of multiple CA or RM workstations to provide support at theater installations having tenants from multiple Services.

o. PKI training plans shall be developed in accordance with applicable Joint and DoD guidance. As a minimum, training plans shall address the training requirements of:

(1). Executives: Explain the impacts of PKI on organizational processes, information systems, and communications networks.

(2). Human users: (including foreign/local nationals and contractor personnel): Address basic user functions including requesting and receiving a signature (i.e., identity) certificate, requesting and receiving encryption certificates, certificate use, certificate replacement/renewal, and requesting certificate revocation.

(3). Application and device-user administrators: Address the same basic user functions as for human users while addressing the unique aspects of managing a PK-enabled application or device.

(4). Application Program Managers: Address the use of PKI and the process of PK-enabling an application.

(5). Developers: Provide information needed by developers to PK-enable new and existing applications.

(6). PKI operators: Provide the information needed by CA and RM operators to operate the PKI in accordance with the DoD CPS.

Appendix L

Information Assurance Vulnerability Alert Process

L-1 **Information Assurance Vulnerability Alerts (IAVAs).** IAVAs are generated whenever a critical vulnerability exists that poses an immediate threat to the DOD for which a corrective measure has been devised, and where acknowledgment and corrective action compliance must be tracked in accordance with Deputy Secretary of Defense (DEPSECDEF) memorandum. Not all identified vulnerabilities and threats will warrant an IAVA. The Commander, Joint Task Force, Computer Network Operations (JTF-CNO), in coordination with the Defense Information Systems Agency (DISA), will issue IAVAs once the IAVA has been pre-coordinated with the JTF-CNO component elements, Service/Agency Computer Emergency Response Teams (CERTs)/Computer Incident Response Teams (CIRTs). Components and supporting elements shall implement EUCOM-directed IAVAs in accordance with EUCOM reporting requirements. In the event of conflicting direction between Service CERT/CIRTs and EUCOM-directed IAVAs, the EUCOM-directed IAVAs will have precedence.

L-2 **USEUCOM IAVA Program Responsibilities.**

a. The TCCC IA Cell is the primary point of contact responsible for IAVA acknowledgment and reporting and will ensure:

1. Upon receipt of the IAVA, the attempt is made to identify, in advance, issues that may impact EUCOM's ability to comply with the IAVA within its AOR. The TCCC will assist the components and supporting elements in prioritizing the implementation of IAVAs on information systems as required. Prioritization of implementation will be determined based on threat and risk to various information system types (i.e. workstations, servers and networks).

2. Components and supporting elements are notified of IAVA release with instructions on IAVA reporting requirements to EUCOM and any information gleaned during the initial analysis of the IAVA by the HQ EUCOM IA analysts. TCCC IA Cell will maintain the Components compliance statistics.

3. Management of HQ EUCOM implementation of Vulnerability Compliance and Tracking System (VCTS) ensuring that all HQ EUCOM elements systems are registered within VCTS and acknowledgement/compliance statistics are being activity completed.

4. Coordinate extension requests from EUCOM Components through the DoD-Cert IAVA Coordinator and JTF-CNO Watch Officer.

b. Components and service elements will report IAVA compliance to their established Service reporting chains and the TCCC IA Cell. Process any extension requests through the appropriate channels to the DAA of the system, but provide any information on major compliance issues to the TCCC IA Cell for DoD and Service-level extension requests.

c. All other EUCOM elements will report IAVA compliance through VCTS. All assets will be registered with VCTS and all System Administrators will have training provided on the system. Extension requests for EUCOM elements will be processed through VCTS.

Appendix M

Terms and Definitions

M-1. **Access**: A specific type of interaction between a subject (i.e., person, process, or input device) and an object (i.e., an information system resource such as a record, file, program, output device) that results in the flow of information from one to the other. Also, the ability and opportunity to obtain knowledge of classified, sensitive unclassified, or unclassified information.

M-2. **Accountability**: The property that enables activities on an information system to be traced to individuals who may then be held responsible for their actions.

M-3. **Accreditation**: A formal declaration by the DAA that the information system is approved to operate in a particular security mode using a prescribed set of safeguards. Accreditation is the official management authorization for operation of an information system and is based on the certification process as well as other management considerations. The accreditation statement affixes security responsibility with the DAA and shows that due care has been taken for security.

M-4. **Assurance**: A measure of confidence that the security features and architecture of an information system accurately mediate and enforce the security policy. If the security features of an information system are relied on to protect classified or sensitive unclassified information and restrict user access, the features must be tested to ensure that the security policy is enforced and may not be circumvented during information system operation.

M-5. **Assurance Levels**: The level of assurance of a public key certificate is the degree of confidence in the binding of the identity to the public keys and privileges. Personnel, physical, procedural and technical security controls contribute to the assurance level of the certificates issued by a certificate management system. The following four levels are defined in the US DoD X.509 Certificate Policy document:

a. Class 2: (Formerly Basic) This level is intended for applications handling information of low value (Unclassified) or protection of system high information in a low to medium risk environment such as SIPRNET. This assurance level does not require that the end user register in person and their cryptography can be software based. Note: DoD will use Class 3 certificates to support Class 2 applications.

b. Class 3: (Formerly Medium) This level is intended for applications handling medium value information in a low to medium risk environment. This assurance level is appropriate for applications that typically require identification of an entity as a legal person, rather than merely as a member of an organization. This assurance level requires that the end user register in person and their cryptography can be software based.

c. Class 4: (Formerly High) This level is intended for applications handling medium to high value information in any environment. These applications typically require identification of an entity as a legal person, rather than merely a member of an organization. This level requires a hardware token for protection of the private key material. This assurance level requires that the end user register in person, and that the cryptography be hardware based.

d. Class 5: This level is intended for applications handling classified information in a high-risk environment (over an open or unprotected network). This assurance level requires National Security Agency (NSA)-approved Type I cryptography.

M-6. **Attack Sensing and Warning (AS&W)**: The detection, correlation, identification and characterization of intentional unauthorized activity, including information system intrusion or attack, across a large spectrum coupled with the notification to command and decision-makers so that an appropriate response can be developed. Attack sensing and warning also includes attack/intrusion related intelligence collection tasking and dissemination; limited immediate response recommendations; and limited potential impact assessments.

M-7. **Attribute**: Information of a particular type. Certificates can contain attributes that convey information about their subjects. An attribute normally has a type, which indicates the class of information it conveys, and one or more values that are the actual information.

M-8. **Attribute Certificate**: A set of attributes of a user together with some other information, rendered un-forgeable by the digital signature created using the private key of the certification authority that issued it.

M-9. **Authentication**: A process used to ascertain the identity of a person, process, or component.

M-10. **Audit**: An independent review and examination of system records and activities to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, and to recommend any indicated changes in controls, policy, or procedures.

M-11. **Audit Trail**: A chronological record of system activities that is sufficient to enable the reconstruction, reviewing, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results.

M-12. **Category**: A grouping of classified or sensitive unclassified information to which an additional restrictive label is applied for signifying that personnel are granted access to the information only if they have formal access approval or other applicable authorization (e.g., proprietary information, for official use only, compartmented information).

M-13. **Certificate**: An information system generated record that ties the user's identification with the user's public key in a trusted bond. The certificate contains the following (*at a minimum*): identity of the issuing Certification Authority and the user, and the user's public key.

M-14. **Certification**: The technical evaluation of an information system's security features and other safeguards, made in support of the accreditation process, which establishes the extent to which a particular information system design and implementation meet a set of specified security requirements.

M-15. **Certification Authority (CA)**: A person trusted and authorized to issue certificates. The CA certifies a user's identity and association with the entity's public key.

M-16. **Certification Practice Statement (CPS)**: A statement of the practices that a certification authority employs in issuing certificates.

M-17. **Certificate Revocation List (CRL)**: An information system generated record that identifies certificates that have been revoked or suspended prior to their expiration dates. It is periodically issued by each certification authority and posted to the directory.

M-18. **Confidentiality**: A security service that protects information from unauthorized disclosure.

M-19. **Common Tier 1 System (CT1S)**: EKMS directory servers providing key management services to the Army Key Management System (AKMS), Air Force Key Management System (AFKMS), Navy Key Distribution System (NKDS), CINCs and Agencies. The CT1S is the layer of key management that exists between the EKMS Central Facility (NSA) and the Services' EKMS accounts residing at the Tier 2 level. The CONUS based components of the CT1S are located at Fort Huachuca, AZ and Kelly AFB, TX. The O-CONUS segment (the Extension Tier 1 Segment or ET1S) is located at Coleman Barracks in Mannheim Germany.

M-20. **Computer Network Defense Service (CNDS) Certification**: An integrated suite of CNDS certification standards, self-assessment and independent-assessment processes, improvement methods, and tools.

M-21. **CNDS Certification Authority (CNDS/CA)**: An entity responsible for certifying CNDS providers, coordinating among assigned CNDS providers, and managing information dissemination supporting CND operations.

M-22. **CND Sensor Grid**: A coordinated constellation of de-centrally owned and implemented intrusion and anomaly detection systems deployed throughout DoD information systems and computer networks. The CND sensor grid is a component of the NETOPS sensor grid.

M-23. **CND Service (CNDS)**: A DoD service provided or subscribed to by owners of DoD information systems or computer networks. The service monitors and analyzes in order to detect unauthorized activity and implements CND operational direction. It also maintains and provides CND situational awareness, and implements CND protect measures.

M-24. **CNDS Providers**: CNDS providers must provide for the coordinated service support of a CNDS/CA. CNDS is commonly provided by a Computer Emergency or Incident Response Team (CERT/CIRT) and may be associated with a Network Operations and Security Center (NOSC).

M-25. **Computer Network Defense (CND)**: Actions taken to protect, monitor, analyze, detect and respond to unauthorized activity with DoD information systems and computer networks. Note: The unauthorized activity may include disruption, denial, degradation, destruction, exploitation, or access to computer networks, information systems or their contents, or theft of information. CND protection employs information assurance actions taken to modify a network configuration or condition in response to a CND alert. CND includes monitoring, analysis, and detection activities, including trend and pattern analysis, as performed by multiple disciplines within the Department of Defense, e.g., network operations, CND Services, intelligence, counterintelligence, and lay enforcement.

M-26. **Data**: A representation of facts, concepts, information, or instructions suitable for communication, interpretation, or processing by humans or by an information system.

M-27. **Data Integrity**: The state that exists when data is unchanged from its source and accidentally or maliciously has not been modified, altered, or destroyed.

M-28. **Data Owner**: The authority, individual, or organization having original responsibility for the data by statute, Executive order, or Directive.

M-29. **Dedicated Security Mode**: A mode of operation wherein all users have the clearance or authorization and need-to-know for all data handled by the information system. If the information system processes special access information, all users require formal access approval. In the dedicated mode, an information system may handle a single classification level and/or category of information or a range of classification levels and/or categories.

M-30. **Denial of Service**: Action or actions that result in the inability of an information system or any essential part to perform its designated mission, either by loss or degradation of operational capability.

M-31. **Designated Approving Authority (DAA)**: The official who has the authority to decide on accepting the security safeguards prescribed for an information system or the official who may be responsible for issuing an accreditation statement that records the decision to accept those safeguards. The DAA must be at an organizational level, have authority to evaluate the overall mission requirements of the information system, and to provide definitive directions to information system developers or owners relative to the risk in the security posture of the information system.

M-32. **Digital Signature**: A transformation of a message using an asymmetric cryptographic system and a hash function such that a person having the initial message and the signer's public key can accurately determine if the transformation was created using the corresponding signer’s private key. In addition, it can be determined if the initial message has been altered since the transformation was made.

M-33**.** **Directory**: The directory is a repository or database of certificates, CRLs, and other information available online to users.

M-34. **Electronic Key Management System (EKMS)**: The EKMS is, by definition, a joint system which performs electronic key generation and distribution functions under strict operator controls. At the user level, a computer workstation called a "Local Management Device/Key Processor (LMD/KP)" supports key generation, management, and distribution requirements using an applications package called "Local COMSEC Management Software (LCMS)." Within the global EKMS structure, the workstation level is referred to as the "Tier 2." All key-management functions are performed under access controls. Depending upon privileges granted by the Service COMSEC Office of Record, workstation operators may or may not be able to generate key locally. Key that cannot be generated locally must be downloaded from the NSA Central Facility (also called the "EKMS Tier Zero"), the Service COMSEC Office of Record (also called the "EKMS Tier 1"); the forward deployed EKMS server located in Mannheim Germany (also called the "Extension Tier 1 Segment or ET1S"), or from another workstation privileged to perform local key generation. Where the term is used, "Tier 3" refers to the data transfer device (AN/CYZ-10 and versions thereof). Currently, all EKMS workstations are standalone devices requiring STU/STE connectivity in order to distribute key.

M-35. **Embedded System**: An embedded system is one that performs or controls a function, either in whole or in part, as an integral element of a larger system or subsystem (e.g., ground support equipment, flight simulators, engine test stands, or fire control systems).

M-36. **Enclave** (a.k.a. Local Computing Environment): Enclaves or local computing environments are the physical or organizational environment under the control of a single authority with a common, uniform security policy. Enclaves are typically defined by geography (Base/Post/Camp/Station) but may also be defined operationally (i.e. JTF AFFOR or ARFOR networks) or logically (DMS). Enclaves are as big (i.e. DISN) or as small (i.e. deployed LAN) as the purview of the controlling authority. All Components and supporting elements shall define the enclaves and boundaries for the information systems under their control and/or responsibility. This includes the interconnect between the USEUCOM portion of the GIG and other networks (i.e. Internet Access Points, NIPRNET/SIPRNET Gateways, STEP sites).

M-37. **Enclave Boundary**: Enclave boundaries are the interconnection between an enclave (local computing environment) and an "untrusted" network or enclave. Enclave boundaries may be the network "De-Militarized Zone (DMZ)" for a Post/Base/Camp/Station or deployed location, the DISN NIPRNET CONUS Gateways, theater Internet Access Points (IAPs) or reachback to STEP Sites.

M-38. **Encryption Certificate**: A certificate containing a public key that is used to encrypt or decrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.

M-39. **Evaluated Products List (EPL)**: A documented inventory of equipments, hardware, software, and/or firmware that have been evaluated against the evaluation criteria found in DoD 5200.28-STD.

M-40. **Formal Access Approval**: Documented approval by a data owner to allow access to a particular category of information.

M-41. **Handled By**: The term "handled by" denotes the activities performed on data in an information system, such as collecting, processing, transferring, storing, retrieving, sorting, transmitting, disseminating, and controlling.

M-42. **Information**: Knowledge such as facts, data, or opinions, including numerical, graphic, or narrative forms regardless of medium.

M-43. **Information Assurance (IA)**: Information Assurance includes all information operations (IO) that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (Note: throughout this appendix, the term IA includes the Key Management Infrastructure or KMI)

M-44. **Information Assurance Red Team**: An independent threat based activity aimed at improving information assurance readiness by emulating a potential adversary's attack or exploitation capabilities.

M-45. **Information Assurance Vulnerability Alert (IAVA)**: The comprehensive distribution process for notifying CINCs, Services and Agencies about vulnerability alerts and countermeasures. The IAVA process requires receipt acknowledgment and provides specific time parameters for implementing appropriate countermeasures depending on the criticality of the vulnerability.

M-46. **Information Operations Condition (INFOCON)**: The INFOCON is a comprehensive defense posture and response based on the status of information systems, military operations, and intelligence assessments of adversary capabilities and intent. The INFOCON system presents a structured, coordinated approach to defend against a computer network attack. INFOCON measures focus on computer network-based protective measures. Each level reflects a defensive posture based on the risk of impact to military operations through the intentional disruption of friendly information systems. INFOCON levels are shown in Appendix H.

M-47. **Information system**: (a.k.a. Automated Information System, or Communications-Computer System) A device or collection of devices that processes or transfers information.

M-48. **Information System Security**: Measures and controls that safeguard or protect an information system against unauthorized (accidental or intentional) disclosure, modification, or destruction of information systems and data, and denial of service. Information system security includes consideration of all hardware and/or software functions, characteristics, and/or features; operational procedures, accountability procedures, and access controls at the central information systems facility, remote information system, and terminal facilities; management constraints; physical structures and devices; and personnel and communication controls needed to provide an acceptable level of risk for the information system and for the data and information contained in the information system. It includes the totality of security safeguards needed to provide an acceptable protection level for an information system and for data handled by an information system.

M-49. **Information System Security Officer (ISSO)**: The person responsible to the DAA for ensuring that security is implemented and provided for throughout the life cycle of an information system from the beginning of the concept development phase through its design, development, operation, maintenance, and disposal.

M-50. **Intelligent Terminal**: A terminal that is programmable, able to accept peripheral devices, able to connect with other terminals or information systems, able to accept additional memory, or which may be modified to have these characteristics.

M-51. **Joint Intertheater COMSEC Package (JICP)**: The JICP is a package of physical keys identified by short titles matched to cryptographic hardware, application, and required operational security level; e.g., USKAT-1019 is used with a KY-57/58 at the SECRET level. The package is globally distributed to accommodate interoperability between supporting and supported CINC forces. The controlling authority for the JICP is the Joint COMSEC Management Office (JCMO) located at MacDill AFB in Florida. The JCMO **"Red Book"** containing all pertinent JICP policies, effective edition messages, and distribution profiles can be accessed at http://157.224.120.250/jcmo.nsf.

M-52. **Key Management Infrastructure (KMI)**: The framework and services that provide for the generation, production, distribution, control, accounting and destruction for all cryptographic key material and public key certificates.

M-53. **Multilevel Security Mode**: A mode of operation that allows two or more classification levels of information to be processed simultaneously within the same system when not all users have a clearance or formal access approval for all data handled by the system.

M-54. **NAG-16**: Under the Transmission Security (TSEC) nomenclature scheme, NAG stands for non-cryptographic (N), operational (A), general publication (G). The long title of NAG-16 is "Field Generation and Over-the-Air Distribution of COMSEC Key in Support of Tactical Operations and Exercises." The document prescribes pre-EKMS techniques to satisfy secure communications requirements without the need to preposition physical key. NAG-16 is published by the National Security Agency and is updated as required. A copy of NAG-16 can be accessed at http://www.eucom.smil.mil/ecj6-i/DIO/NAG-16/nag16e.htm.

M-55. **Need-to-know**: A determination made in the interest of U.S. national security (by the custodian of classified or sensitive unclassified information) that a prospective recipient has a requirement for access to the information in order to perform official tasks or services.

M-56. **Network**: Networks are the interconnections between enclaves and are viewed as “untrusted” resources from the perspective of the enclave. Networks include, but are not limited to, NIPRNET and SIPRNET.

M-57. **Non-Repudiation**: Strong and substantial evidence of the identity of the signer of a message, sufficient to prevent a party from successfully denying the origin, submission or delivery of the message and the integrity of its contents.

M-58. **Private Key**: The part of a key pair to be safeguarded by the owner. A private key is used to encrypt a digital signature. Private keys are used to decrypt information, including key encryption keys during key exchange. It is computationally infeasible to determine a private key given the associated public key.

M-59. **Public Key**: The part of a key pair released to the public. The signer's public key is used to verify a digital signature. Public keys are used for encryption, including the encryption of privacy keys during key exchange.

M-60. **Public Key-Enabled (PKE) Application**: A software application that uses public key technology to: authenticate its users, ensure information is not changed or modified either during transmission or storage, hold users responsible and accountable for their actions and representation, or encrypt information between parties where prior arrangement is not practical.

M-61. **Public Key-Enabled (PKE) Device**: A devise that uses public key technology to authenticate its interactions with other PK-enabled devices, authenticate users requesting services, provide integrity and/or confidentiality for information it transmits and receives, or otherwise provide security protection for its operation.

M-62. **Purge**: Removal of sensitive data from an information system (including from information system storage devices and other peripheral devices with storage capacity) at the end of a period of processing. Removal is performed in a manner that ensures the data may not be reconstructed. An information system must be disconnected from any external network before a purge.

M-63. **Registration Authority (RA)**: Entity responsible to the Certification Authority (CA) for identification and authentication of certificate owners. RAs do not sign or directly revoke certificates. The term "RA" is used with the existing DoD Class 3 PKI; the terms local registration authority (LRA) and organizational registration authority (ORA) are also used.

M-64. **Registration Manager (RM)**: KMI term for role granted to those KMI users responsible for authenticating and submitting identity credential requests. This role is similar in scope to the role of RA in the existing DoD Class 3 PKI. RMs are also able to request key establishment certificates, revoke certificates and request recovery of a key establishment key.

M-65. **Root Certification Authority**: The Root CA is a trusted entity responsible for establishing and managing a PKI domain by issuing CA certificates to entities authorized and trusted to perform CA functions.

M-66. **Risk Analysis**: An analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of occurrence.

M-67. **Risk Index**: The disparity between the minimum clearance or authorization of information system users and the maximum sensitivity (e.g., classification and categories) of data handled by the information system.

M-68. **Security Mode**: A mode of operation in which the DAA accredits an information system to operate within the parameters of one or more of the four security modes (dedicated, system high, multilevel, and partitioned). Consideration is also given to user clearance levels, formal access requirements, and the range of sensitive information permitted on the information system.

M-69. **Security Safeguards**: The protective measures and controls prescribed to meet the security requirements specified for an information system. These safeguards may include, but are not necessarily limited to, hardware and software security features; operation procedures; accountability procedures; access and distribution controls; management constraints; personnel security; and physical structures, areas, and devices.

M-70. **Signature Certificate**: A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.

M-71. **SMI**: The framework and services that provide for the overall security of an information infrastructure. SMI includes KMI plus additional services associated with security applications, the common operating environment (e.g., operating system security), software downloading, auditing, Intrusion Detection, and password management.

M-72. **Special Access Program**: Any program imposing need-to-know or access controls beyond those normally required for access to Confidential, Secret, or Top Secret information. Such a program includes, but is not limited to, special clearance of investigative requirements, special designation of officials authorized to determine need-to-know, or special lists of persons determined to have a need-to-know.

M-73. **Special Enclave**: DoD information systems and/or computer networks with special security requirements (e.g., Special Access Programs (SAP), Special Access Requirements (SAR) and designated as Special Enclave by the ASD(C3I).

M-74. **System High Security Mode**: A mode of operation wherein all users having access to the information system possess a security clearance or authorization, but not necessarily a need-to-know, for all data handled by the information system. If the information system processes special access information, all users must have formal access approval.

M-75. **Vulnerability Analysis and Assessment**: In information operations, a systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.